

Школа – Инженерная школа информационных технологий и робототехники Направление подготовки – 15.03.04 «Автоматизация технологических процессов и производств»
 Отделение школы (НОЦ) – Отделение автоматизации и робототехники

БАКАЛАВРСКАЯ РАБОТА

Тема работы
Построение двоичных регистров сдвига с линейной обратной связью.

УДК 004.314.4

Студент

Группа	ФИО	Подпись	Дата
3-8Т52	Скоробогатов Кирилл Дмитриевич		

Руководитель ВКР

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Литвинов Рудольф Викторович	к.э.н., доцент		

КОНСУЛЬТАНТЫ ПО РАЗДЕЛАМ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОСГН ШБИП	Конотопский В. Ю.	к.э.н., доцент		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент ООД ШБИП	Матвиенко В. В.			

ДОПУСТИТЬ К ЗАЩИТЕ:

Руководитель ООП	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Воронин А. В.	к.т.н., доцент		

Запланированные результаты обучения по направлению «Автоматизация
технологических процессов и производств»

Код результата	Результат обучения (выпускник должен быть готов)
Профессиональные компетенции	
P1	Использовать основные знания в области математических и естественных наук для решения научных и инженерных задач в области анализа, синтеза, проектирования, производства и эксплуатации систем автоматизации технологических процессов и производств. Уметь сочетать теоретические и практические навыки и методы решения инженерных задач.
P2	Применять полученные знания для определения, формулирования и решения инженерных задач при разработке, производстве и эксплуатации систем автоматизации технологических процессов и производств с использованием передовых научно-технических знаний и достижений мирового уровня, современных инструментальных и программных средств.
P3	Уметь выбирать и применять соответствующие аналитические методы проектирования систем автоматизации технологических процессов и обосновывать экономическую целесообразность решений.
P4	Иметь представление о передовом отечественном и зарубежном опыте в области теории, проектирования, производства и эксплуатации систем автоматизации технологических процессов и производств.
P5	Уметь находить необходимую литературу, базы данных и другие источники информации для автоматизации технологических процессов и производств.
P6	Уметь выбирать и использовать подходящее программно-техническое оборудование, оснащение и инструменты для решения задач автоматизации технологических процессов и производств.
P7	Уметь планировать и проводить эксперимент, интерпретировать данные и их использовать для ведения инновационной инженерной деятельности в области автоматизации технологических процессов и производств.
Универсальные компетенции	
P8	Владеть иностранным языком на уровне, позволяющем работать в интернациональной среде с пониманием культурных, языковых и социально – экономических различий.
P9	Эффективно работать индивидуально и в качестве члена и руководителя группы. Быть готовым нести ответственностью за риски в работе коллектива при решении инженерных задач в области автоматизации технологических процессов и производств, демонстрировать при этом готовность следовать профессиональной этике и нормам.
P10	Иметь широкую эрудицию, в том числе знание и понимание современных общественных и политических проблем, вопросов безопасности и охраны здоровья сотрудников, ответственности за инженерную деятельность, влияния инженерных решений на социальный контекст и окружающую среду, юридических аспектов.
P11	Понимать необходимость и уметь самостоятельно учиться и повышать квалификацию в течение всего периода профессиональной деятельности.

Министерство науки и высшего образования Российской Федерации
 федеральное государственное автономное
 образовательное учреждение высшего образования
 «Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа – Инженерная школа информационных технологий и робототехники Направление подготовки (специальность) – 15.03.04 «Автоматизация технологических процессов и производств»

Уровень образования – Бакалавриат

Отделение школы (НОЦ) - Отделение автоматизации и робототехники Период выполнения осенний / весенний семестр 2019 /2020 учебного года

Форма представления работы:

БАКАЛАВРСКАЯ РАБОТА

(бакалаврская работа, дипломный проект/работа, магистерская диссертация)

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	27.05.2020
--	------------

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
	Основная часть	60
	Финансовый менеджмент, ресурсоэффективность и ресурсбережение	20
	Социальная ответственность	20

СОСТАВИЛ:

Руководитель ВКР

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Литвинов Р.В.	к.ф.-м.н.		

СОГЛАСОВАНО:

Руководитель ООП

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Воронин А. В.	к.т.н., доцент		

Министерство науки и высшего образования Российской Федерации
 федеральное государственное автономное
 образовательное учреждение высшего образования
 «Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа – Инженерная школа информационных технологий и робототехники Направление подготовки (специальность) – 15.03.04 «Автоматизация технологических процессов и производств»

Отделение школы (НОЦ) – Отделение автоматизации и робототехники

УТВЕРЖДАЮ:

Руководитель ООП

_____ Воронин А. В.
 (Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ

на выполнение выпускной квалификационной работы

В форме:

БАКАЛАВРСКАЯ РАБОТА

(бакалаврской работы, дипломного проекта/работы, магистерской диссертации)

Студенту:

Группа	ФИО
3-8Т52	Скоробогатову Кириллу Дмитриевичу

Тема работы:

Построение двоичных регистров сдвига с линейной обратной связью.	
Утверждена приказом директора (дата, номер)	28.02.2020 №59-64/с

Срок сдачи студентом выполненной работы:	27.05.2020
--	------------

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе <i>((наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т. д.); вид сырья или материал изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т. д.).</i>	Объект исследования – Двоичный регистр сдвига с линейной обратной связью для генерации бинарной рекуррентной последовательности 16-го порядка. Регистр предназначен для генерации бинарной последовательности максимального периода (PN-последовательности). Временной слот одного бита последовательности 50 нс.
---	--

<p>Перечень подлежащих исследованию, проектированию и разработке вопросов <i>(аналитический обзор по литературным источникам с целью выяснения достижений мировой науки техники в рассматриваемой области; постановка задачи исследования, проектирования, конструирования; содержание процедуры исследования, проектирования, конструирования; обсуждение результатов выполненной работы; наименование дополнительных разделов, подлежащих разработке; заключение по работе).</i></p>	<ol style="list-style-type: none"> 1. Аналитический обзор современного состояния разработки и производства высокоскоростных регистров сдвига. 2. Основные теоретические положения линейных рекуррентных последовательностей. 3. Рекуррентные последовательности и регистры сдвига. 4. Линейные рекуррентные последовательности над бинарным полем и регистры сдвига с линейной обратной связью. 5. Выбор характеристического (примитивного) полинома, позволяющего минимизировать схемную реализацию регистра. 6. Разработка функциональной схемы регистра. 7. Разработка принципиальной электрической схемы и выбор вектора начального состояния. 8. Таблица генерации PN-последовательности. Анализ ее статистических свойств на основе различных тестов. 9. Заключение по работе.
<p>Перечень графического материала <i>(с точным указанием обязательных чертежей)</i></p>	<ol style="list-style-type: none"> 1. Функциональная схема регистра сдвига с линейной обратной связью. 2. Принципиальная электрическая схема регистра сдвига с линейной обратной связью. 3. Таблица генерации бинарной последовательности. 4. Гистограмма распределения элементов последовательности. 5. Распределение на плоскости. 6. Автокорреляционная функция. 7. Графический спектральный тест.
<p>Консультанты по разделам выпускной квалификационной работы <i>(с указанием разделов)</i></p>	
<p>Раздел</p>	<p>Консультант</p>
<p>1 Основная часть</p>	<p>Доцент ОАР ИШИТР, к.ф.-м.н., Литвинов Р. В.</p>
<p>2 Финансовый менеджмент, ресурсоэффективность и ресурсосбережение</p>	<p>Доцент ОСТН ШБИП, к.э.н., Конотопский В.Ю.</p>
<p>3 Социальная ответственность</p>	<p>Ассистент ООД ШБИП Матвиенко В. В.</p>
<p>Названия разделов, которые должны быть написаны на русском и иностранном языках:</p>	

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	07.04.2020
--	------------

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Литвинов Р. В.	к.ф.-м.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
З-8Т52	Скоробогатов Кирилл Дмитриевич		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА

«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
З-8Т52	Скоробогатову Кириллу Дмитриевичу

Школа		Отделение школы (НОЦ)	
Уровень образования	Бакалавриат	Направление/специальность	15.03.04 «Автоматизация технологических процессов и производств»

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих	Использовать действующие ценники и договорные цены на потребляемые материальные и информационные ресурсы, а также указанную в МУ величину тарифа на электроэнергию
2. Нормы и нормативы расходования ресурсов	—
3. Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования	Действующие ставки единого социального налога и НДС (см. МУ)
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Оценка коммерческого потенциала, перспективности и альтернатив проведения НИ с позиции ресурсоэффективности и ресурсосбережения	Оценка готовности полученного результата к выводу на целевые рынки, краткая характеристика этих рынков
2. Планирование и формирование бюджета научных исследований	Построение плана-графика выполнения ВКР, составление соответствующей сметы затрат, расчет величины НДС и цены результата ВКР
3. Определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования	Качественная и количественная характеристика экономического и др. видов эффекта от внедрения результата, определение эффективности внедрения

Перечень графического материала.
1. Оценка конкурентоспособности технических решений 2. Матрица SWOT 3. Альтернативы проведения НИИ 4. График проведения и бюджет НИИ - <u>выполнить</u> Оценка ресурсной, финансовой и экономической эффективности НИИ - <u>выполнить</u>

Дата выдачи задания для раздела по линейному графику	
---	--

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОСГН ШБИП	Конотопский Владимир Юрьевич	к. э. н., доцент		29.02.2020 г.

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
3-8Т52	Скоробогатов Кирилл Дмитриевич		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА «СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
3-8Т52	Скоробогатову Кириллу Дмитриевичу

Школа	ИШИТР	Отделение (НОЦ)	ОАР
Уровень образования	Бакалавриат	Направление/специальность	15.03.04 «Автоматизация технологических процессов и производств»

Тема ВКР:

Построение двоичных регистров сдвига с линейной обратной связью.	
Исходные данные к разделу «Социальная ответственность»:	
1. Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика, рабочая зона) и области его применения	Двоичный регистр сдвига с линейной обратной связью для генерации бинарной рекуррентной последовательности 16-го порядка. Регистр предназначен для генерации бинарной

	последовательности максимального периода (PN- последовательности).
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Правовые и организационные вопросы обеспечения безопасности: <input type="checkbox"/> специальные правовые нормы трудового законодательства; <input type="checkbox"/> организационные мероприятия при компоновке рабочей зоны.	1. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 27.12.2018) 2. ГОСТ 12.2.032-78 ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования.
2. Производственная безопасность: <input type="checkbox"/> анализ выявленных вредных и опасных факторов; <input type="checkbox"/> обоснование мероприятий по снижению воздействия.	К вредным и опасным факторам относятся: Уровень шума на рабочем месте Электрический ток Уровень электромагнитных излучений Микроклимат воздуха рабочей зоны Освещенность рабочей зоны
3. Экологическая безопасность:	Оказывается, воздействие на литосферу при утилизации электронных компонентов
4. Безопасность в чрезвычайных ситуациях:	Наиболее вероятной ЧС является пожар

Дата выдачи задания для раздела по линейному графику	
--	--

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент ООД	Матвиенко Владимир Владиславович			

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
3-8Т52	Скоробогатов Кирилл Дмитриевич		

РЕФЕРАТ

Пояснительная записка содержит 77 страниц машинописного текста, 12 таблиц, 20 рисунок, 1 список использованных источников из 31 наименований, 7 приложения.

Ключевые слова: Регистр сдвига с линейной обратной связью, PN – последовательность, вектор начального состояния, примитивный полином, статический тест.

Объектом исследования является двоичный регистр сдвига с линейной обратной связью для генерации бинарной рекуррентной последовательности 16-го порядка.

Цель работы – исследование однородных линейных рекуррентных последовательностей над бинарным полем. Построение последовательностей максимальной длины при помощи регистров сдвига с линейной обратной связью.

В данном проекте был выбран характеристический (примитивный) полином, позволяющий минимизировать схемную реализацию регистра, разработана функциональная и принципиальная электрическая схемы регистра сдвига с линейной обратной связью, построена таблица генерации PN-последовательности.

Регистры сдвига обширно применяются для выполнения всевозможных временных преобразований цифровой информации: последовательное скопление поочередной цифровой информации с дальнейшей одновременной выдачей (преобразование поочередной цифровой информации в параллельный код) или же одновременный прием (параллельный прием) информации с дальнейшей поочередной выдачей (преобразование параллельного кода в последовательный).

Содержание

Обозначения и сокращения	13
Введение.....	14
1.Регистр сдвига	15
1.1 Аналитический обзор современного состояния разработки и производства высокоскоростных регистров сдвига	15
1.2 Основные теоретические положения линейных рекуррентных последовательностей	18
1.3 Рекуррентные последовательности и регистры сдвига	21
1.4 Линейные рекуррентные последовательности над бинарным полем и регистры сдвига с линейной обратной связью	24
1.5 Исследование свойств последовательностей, генерируемых РСЛОС ...	28
1.5.1 Гистограмма распределения элементов последовательности.....	29
1.5.2 Распределение на плоскости.....	30
1.5.3. Автокорреляционная функция	31
1.5.4. Графический спектральный тест.....	32
2. Построение таблицы и схем.....	34
2.1 Выбор характеристического (примитивного) полинома, позволяющего минимизировать схемную реализацию регистра	34
2.2 Разработка функциональной схемы регистра	35
2.3 Разработка принципиальной электрической схемы и выбор вектора начального состояния	35
2.4 Таблица генерации PN-последовательности. Анализ ее статистических свойств на основе различных свойств	36
2.4.1 Гистограмма распределения элементов последовательности.....	37
2.4.2 Распределение на плоскости.....	37
2.4.3 Автокорреляционная функция	38
2.4.3 Графический спектральный тест.....	38
3. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение..	40
3.1 Организация и планирование работ.....	40

3.1.1 Продолжительность этапов работ	41
3.2 Расчет сметы затрат на выполнение проекта	45
3.2.1 Расчет затрат на материалы	45
3.2.2 Расчет заработной платы.....	46
3.2.3 Расчет затрат на социальный налог	47
3.2.4 Расчет затрат на электроэнергию	47
3.2.5 Расчет амортизационных расходов.....	48
3.2.6 Расчет расходов, учитываемых непосредственно на основе платежных (расчетных) документов (кроме суточных)	49
3.2.7 Расчет прочих расходов	50
3.2.8 Расчет общей себестоимости разработки.....	50
3.2.9 Расчет прибыли	51
3.2.10 Расчет НДС	51
3.2.11 Цена разработки НИР	51
3.3 Оценка экономической эффективности проекта	51
4. Социальная ответственность	52
Введение к разделу	52
4.1. Правовые и организационные вопросы обеспечения безопасности.	53
4.2. Производственная безопасность	56
4.2.1. Уровень шума на рабочем месте.....	57
4.2.2. Электрический ток.....	57
4.2.3. Уровень электромагнитных излучений	58
4.2.4. Микроклимат воздуха рабочей зоны	60
4.2.5. Освещенность рабочей зоны	61
4.3. Электрический ток	61
4.4. Экологическая безопасность.....	62
4.4.1. Анализ влияния объекта исследования на окружающую среду	62
4.4.2. Обоснование мероприятий по защите окружающей среды	63
4.5. Безопасность в чрезвычайных ситуациях	64
4.5.1. Анализ вероятных ЧС, которые может инициировать объект	

исследований	64
4.5.2. Обоснование мероприятий по предотвращению ЧС и разработка порядка действия в случае возникновения ЧС	65
Вывод по разделу	66
Заключение	67
Список использованных источников	68
Приложение А	71
Приложение Б	72
Приложение В.....	73
Приложение Г	74
Приложение Д.....	75
Приложение Е	76
Приложение Ж.....	77

Обозначения и сокращения

GPS - спутниковая система навигации, обеспечивающая измерение расстояния, времени и определяющая местоположение во всемирной системе координат.

CRC - (циклический избыточный код) иногда называемый также контрольным кодом. Это вычисленное на основе исходного передаваемого сообщения число, которое передаётся вместе с самим сообщением и служит для контроля его безошибочной передачи.

CDMA - это стандарт связи второго поколения, являющийся аналогом GSM.

TDMA - (множественный доступ с разделением по времени) — способ использования радиочастот, когда в одном частотном интервале находятся несколько абонентов, разные абоненты используют разные временные слоты (интервалы) для передачи.

RTC - часы реального времени, электронная схема, предназначенная для учёта хронометрических данных. представляет собой систему из автономного источника питания и учитывающего устройства.

Введение

Объектом исследования является двоичный регистр сдвига с линейной обратной связью для генерации бинарной рекуррентной последовательности 16-го порядка.

В данном проекте был выбран характеристический (примитивный) полином, позволяющий минимизировать схемную реализацию регистра, разработана функциональная и принципиальная электрическая схемы регистра сдвига с линейной обратной связью, построена таблица генерации PN-последовательности.

Регистры сдвига обширно применяются для выполнения всевозможных временных преобразований цифровой информации: последовательное скопление поочередной цифровой информации с дальнейшей одновременной выдачей (преобразование поочередной цифровой информации в параллельный код) или же одновременный прием (параллельный прием) информации с дальнейшей поочередной выдачей (преобразование параллельного кода в последовательный).

1.Регистр сдвига

1.1 Аналитический обзор современного состояния разработки и производства высокоскоростных регистров сдвига

Регистры сдвига (последовательные регистры) представляют собой цепочку разрядных схем, связанных цепями переноса. [1].

Быстродействие регистра соответствует минимальному значению периода следования сигналов сдвига и определяется в основном переходными процессами заряда и разряда конденсатора.

Регистры - наиболее обширно употребляемые блоки числовых устройств. Они выполняют процедуру с рядами связанных значений, составляющих переменную. Над значениями осуществляется ряд операций: вноска, хранение, сдвиг в разрядной последовательности. При помощи регистров возможно организовывать методы видоизменения данных из любой разновидности в иную (алгоритмического кода переменной в единовременный и т.д.), и вдобавок многие логические функции (поразрядная логическая совокупность и нарастание и т.п.). Они используются в свойстве управляющих и фиксирующих устройств, дивизоров колебания, генераторов.

Регистры сдвига применяются в GPS. Каждый спутник непрерывно передает последовательность, генерируемую регистром сдвига, длиной 10 бит. По полученной части последовательности приемник определяет, в какое время принятый сигнал был отправлен с конкретного спутника. Путем сравнения задержки времени от различных спутников, приемник может триангулировать свое положение (существует также режим GPS, использующий регистр сдвига длиной 1024 бита).

Генерируемые регистрами сдвига последовательности позволяют их применять в кодах коррекции ошибок, например, CRC (циклический избыточный код) или коды Рида-Соломона (применялись для кодирования видеоизображений для космического корабля).

Одним из самых известных применений последовательностей регистров сдвига являются CDMA телефоны (множественный доступ с кодовым

разделением). Вместо применяемого в классической сотовой связи временного разделения каналов (TDMA), CDMA использует кодовое разделение на основе последовательности регистра сдвига максимальной длины. CDMA применяется в большинстве сетей 3G.

Кроме того, на сегодняшний день существует возможность проверки многочленов на их примитивность при помощи таких систем, как Mathematica и языка программирования Wolfram Language [2].

На сегодняшний день активно исследуются возможности использования регистров сдвига с нелинейной обратной связью с клеточными автоматами.

Регистры сдвига с линейной обратной связью (РСЛОС) могут быть реализованы аппаратными средствами, собственно, что разрешает применять их для быстрой генерации псевдослучайной последовательности, к примеру, при расширении диапазона способом прямой последовательности или же для генерации шумового сигнала.

Программные реализации РСЛОС довольно медленны и работают скорее, в случае если они написаны на Ассемблере. Одно из решений – параллельное использование 16-ти РСЛОС. В такой схеме применяется массив слов, величина которого равна длине регистра сдвига, а каждый бит слова относится к собственному РСЛОС. Так как используются одинаковые номера отводных последовательностей, то это имеет возможность предоставить заметный выигрыш в производительности генератора.

В 1997 году в Японии был разработан генератор «Вихрь Марсенна» - витковый регистр сдвига с обобщенной отдачей с периодом $2^{19937}-1$, равный числу Марсенна M_{19937} . Его характеристический многочлен насчитывает более 100 членов. Скорость работы в 2-3 раза выше, чем у обычного РСЛОС, но генератор, к сожалению, оказался не криптостойким.

Большое распространение регистры сдвига получили в световой индикации, за счет возможности управления большим числом светодиодов имея малое число входов.

Одной из наиболее популярных микросхем 8-битного сдвигового

регистра с 3-мя состояниями является 74НС595 (отечественный аналог - КР1564ИР52) (см. рисунок 1.1).

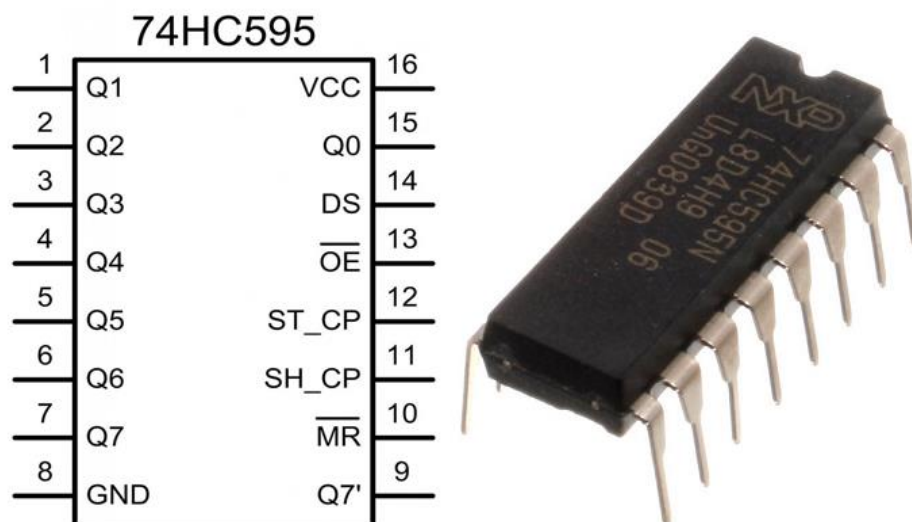


Рисунок 1.1 – Схема и внешний вид микросхемы 74НС595

Параметры данной микросхемы:

Напряжение питания: 2-6 В;

Ток потребления ($I_{\text{пот}}$): 0,08 мА;

Время задержки (t_3): 34 нс;

Частота коммутации (f_{MAX}): 28 МГц

1.2 Основные теоретические положения линейных рекуррентных последовательностей

Пусть k – натуральное число, а $a, a_0, a_1, \dots, a_{k-1}$ – заданные элементы конечного поля F_q . Последовательность s_0, s_1, \dots элементов поля F_q , удовлетворяющая соотношению:

$$s_{n+k} = a_{k-1} s_{n+k-1} + a_{k-2} s_{n+k-2} + \dots + a_0 s_n + a; n = 0, 1, \dots \quad (1.1)$$

называется *линейной рекуррентной последовательностью (k -го порядка)* над полем F_q . Первые члены s_0, s_1, \dots, s_{k-1} однозначно определяют всю последовательность и называются ее начальными значениями.

Если $a = 0$, то линейное рекуррентное соотношение (1.1) называется однородным, если $a = 1$ – неоднородным.

Свойства линейных рекуррентных последовательностей:

1. Любая последовательность, генерируемая РСЛОС, является периодической, т.е. $s_{n+T} = s_n$ для некоторого числа T . Период полученной битовой последовательности называют *периодом регистра*.

2. РСЛОС длины n не может иметь более чем 2^n начальных состояний, поэтому период последовательности не превышает значения $2^n - 1$.

3. Если старший коэффициент последовательности $a_{k-1} = 0$, то последовательность имеет *передпериод*, то есть соотношение $s_{n+T} = s_n$ начинает выполняться с некоторого номера $n \geq \lambda$, где λ – предпериод.

4. Если $a_{k-1} = 1$, то генерированная последовательность называется *неособой*. Она начинается сразу со своей периодической части.

5. Если минимальный многочлен последовательности неприводимый над полем F_q и имеет степень n , то период последовательности T является делителем числа $2^n - 1$.

Ненулевая выходная последовательность регистра сдвига с линейной обратной связью с характеристическим многочленом $f(x)$ тогда и только тогда является последовательностью максимального минимального периода (*PN-последовательностью*), когда многочлен $f(x)$ примитивен.

Многочлен $f \in F_q[x]$ степени $m \geq 1$ называется *примитивным многочленом*

над полем F_q , если он является минимальным многочленом над F_q некоторого примитивного элемента расширения $F_q m$ поля F_q .

Для построения PN -последовательности k -го порядка необходимо:

- построить поле многочленов над полем F_q со степенью, не превышающей k ;
- найти неприводимый многочлен;
- построить расширение этого поля $F_q m$, в качестве образующего элемента которого используется некоторый корень этого многочлена.

Свойства PN -последовательности:

1. Каждая PN -последовательность – чисто периодическая;
2. Для битовых PN -последовательностей (с примитивным минимальным многочленом) характерна *сбалансированность* (появление одинакового числа 0 и 1 на периоде);
3. На каждом периоде PN -последовательности любая ненулевая подпоследовательность длины r появится только один раз.

В таблице 1.1 представлены примеры примитивных полиномов [3].

Таблица 1.1. Примеры примитивных полиномов

Биты, n	Пример примитивного многочлена	Период, 2^n-1	Число примитивных многочленов
2	x^2+x+1	3	1
3	x^3+x^2+1	7	2
4	x^4+x^3+1	15	2
5	x^5+x^3+1	31	6
6	x^6+x^5+1	63	6
7	x^7+x^6+1	127	18
8	$x^8+x^6+x^5+x^4+1$	255	16
9	x^9+x^5+1	511	48
10	$x^{10}+x^7+1$	1023	60
11	$x^{11}+x^9+1$	2047	176
12	$x^{12}+x^{11}+x^{10}+x^4+1$	4095	144
13	$x^{13}+x^{12}+x^{11}+x^8+1$	8191	630
14	$x^{14}+x^{13}+x^{12}+x^2+1$	16383	756
15	$x^{15}+x^{14}+1$	32767	1800
16	$x^{16}+x^5+x^3+x^2+1$	65535	2048

1.3 Рекуррентные последовательности и регистры сдвига

Регистры сдвига строятся из конструктивных элементов, следующих четырех типов: сумматор, усилитель (умножает на элемент a), увеличитель (прибавляет элемент a), элемент задержки (триггер).

Для реализации регистра сдвига применяются RS-, D- или JK-триггеры. Управление регистром сдвига производится подачей тактового импульса. Двоичные числа, хранящиеся в триггерах, сдвигаются от одного триггера к другому на каждый импульс тактового сигнала. Обычно, для формирования этого сигнала используется стандартный высокостабилизированный генератор необходимой частоты. Ключевым параметром такого генератора обычно является выходная частота и стабильность, которая выражается в частях на миллион (parts per million, ppm). Типовое значение стабильности генератора составляет ± 50 или ± 100 ppm [4].

В сдвиговых регистрах все триггеры объединены в последовательную цепочку (выход каждого предыдущего триггера соединен со входом D следующего триггера). Тактовые входы всех триггеров (C) соединены меж собой. В итоге подобный триггер имеет возможность рассматриваться как линия задержки, входной сигнал которой поочередно перезаписывается из триггера в триггер по фронту тактового сигнала C. Информационные входы и выходы триггеров могут быть выведены наружу, а могут и не выводиться - в зависимости от функции, производимой регистром.

По разновидности операций над символами отличают регистры массивные (памяти, занесения), предназначенные для приема и вывода значений, и пошаговые.

По численности входов различают цело- и несколькофазные регистры. В единогофазных регистрах переменная подается на всякий разряд только лишь по единому выходу связи (прямому либо обратному), а в двухфазных - по двум ходам передачи.

По числу импульсов управления, нужных для внесения шифра значения, отличают четырех-, пяти- и многосигнальные (d -тактные) регистры.

По методу взятия и передачи переменных различают методические, единовременные и одновременно-ортодоксальные регистры. В единовременных списках сохранения и выдача слов реализуется по всем битам синхронно.

Основной режим работы регистров — это сдвиг разрядов кода, записанного в эти триггеры, то есть по тактовому сигналу содержимое предшествующего триггера переписывается в следующий по порядку в цепочке триггер. Код, записанный в регистре, с каждым тактом сдвигается на один разряд в сторону старших разрядов или же в сторону младших разрядов, собственно, что и дало название регистрам данного типа.

На схемах регистра сдвига обозначают буквами *RG*. Для регистров сдвига указывается также направление сдвига:

- → вправо (основной режим, который есть у всех сдвиговых регистров);
- ← влево (этот режим есть только у некоторых, реверсивных сдвиговых регистров);
- ↔ реверсивный (двунаправленный), т.е. записанную информацию можно сдвигать по линейке триггеров вправо или влево. Для включения режима сдвига предусматривают специальный управляющий вход.

Направление сдвига отражают внутреннюю структуру регистров сдвига и перезапись сигналов поочередно по цепочке триггеров. При этом триггеры, нумеруются слева направо, к примеру, от 0 до 7 (или от 1 до 8) для 8-разрядных регистров. В итоге сдвиг информации регистром вправо представляет собой сдвиг в сторону разрядов, имеющих большие номера, а сдвиг влево в сторону разрядов, имеющих меньшие номера.

Впрочем, в любом двоичном числе слева расположены старшие разряды, а справа - младшие разряды. В следствии этого сдвиг двоичного числа вправо станет сдвигом в сторону младших разрядов, а сдвиг влево в сторону старших разрядов.

О такой особенности необходимо помнить разработчику цифрового

прибора.

На рисунке 1.3.1 представлен пример построения регистра сдвига вправо.

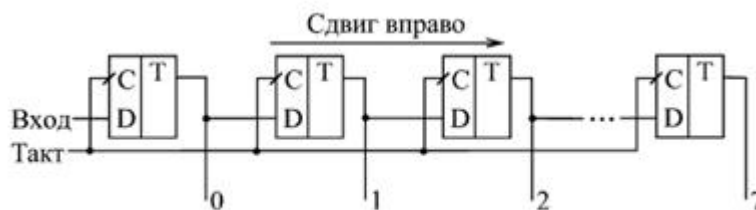


Рисунок 1.3.1 – Пример регистра сдвига вправо

Регистры сдвига могут выполнять функции хранения и преобразования информации. Они применяются для построения умножителей и делителей чисел двоичной системы счисления, т.к. сдвиг двоичного числа влево на один разряд соответствует умножению его на два, а сдвиг вправо - делению на два.

Регистры сдвига широко используются для выполнения различных временных преобразований цифровой информации: последовательное накопление последовательной цифровой информации с последующей одновременной выдачей (преобразование последовательной цифровой информации в параллельный код) или одновременный прием (параллельный прием) информации с последующей последовательной выдачей (преобразование параллельного кода в последовательный).

Регистры сдвига могут применяться в качестве элементов задержки сигнала, представленного в цифровой форме: регистры с поочередным приемом (вводом) и выводом выполняют задержку передачи информации на $m+1$ тактов ($m+1$ - число разрядов регистра) машинного времени.

1.4 Линейные рекуррентные последовательности над бинарным полем и регистры сдвига с линейной обратной связью

Линейные рекуррентные последовательности можно получать с помощью *регистров сдвига с обратной связью*. Это электронные переключательные схемы специального вида, перерабатывающие информацию.

Регистр сдвига с обратной связью строится путем соединения конечного числа конструктивных элементов в замкнутую цепь таким образом, что никакие два выхода не присоединяются друг к другу.

На рисунке 1.4.1 представлен общий вид регистра сдвига с обратной связью [5].

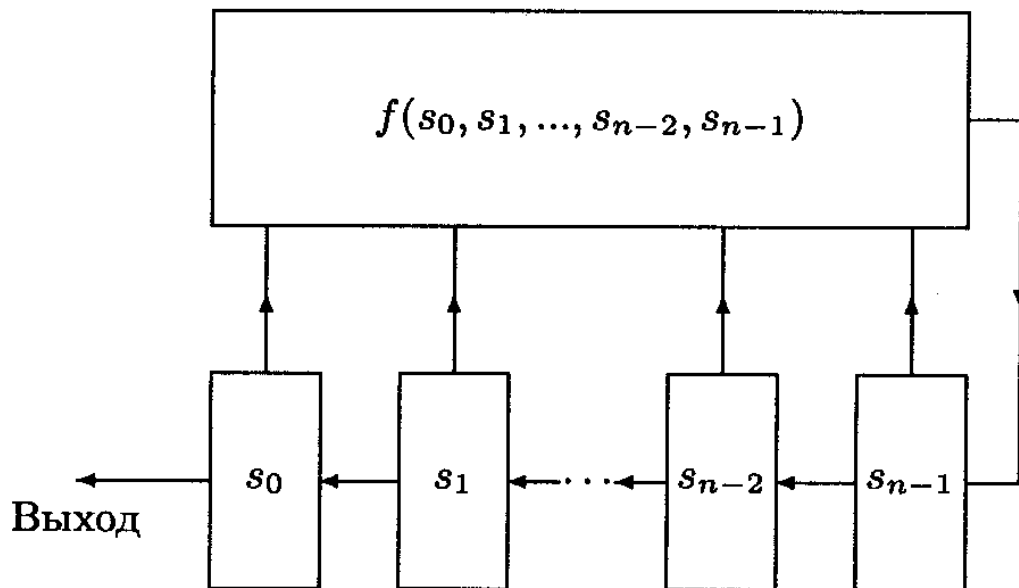


Рисунок 1.4.1 – Общий вид регистра сдвига с обратной связью

Функция f называется функцией обратной связи регистра. Она является булевой функцией и может легко быть построена из элементарных логических функций. После первого такта работы регистр сдвига выдаст s_0 и перейдет в состояние $\{s_1, s_2, \dots, s_n\}$, где $s_n = f\{s_0, s_1, \dots, s_{n-1}\}$. Продолжая таким образом, регистр сдвига генерирует бесконечную последовательность $\{s_n\}_{i \geq 0}$. Функция f в общем случае нелинейная.

На рисунке 1.4.2 представлен пример регистра сдвига с линейной обратной связью.

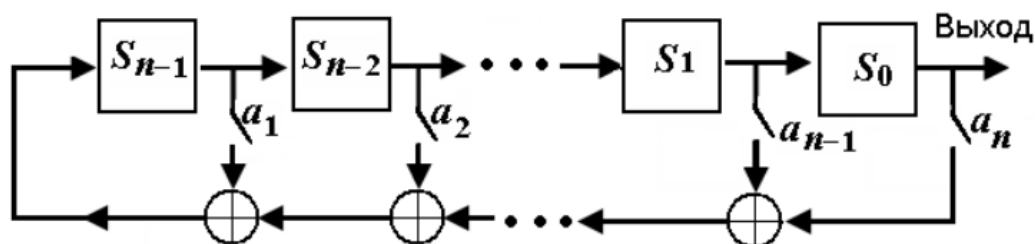


Рисунок 1.4.2 – Пример регистра сдвига с линейной обратной связью

Функцией обратной связи для РСЛОС является операция XOR над некоторыми его битами (*отводами*).

РСЛОС работает в дискретные моменты времени, в каждый из которых выполняются следующие операции:

- содержание ячейки S_0 «выталкивается» из регистра и формирует очередной элемент генерируемой последовательности;
- содержание ячейки S_i перемещается в ячейку S_{i-1} , $i=0,1,\dots,n-1$;
- новое содержание самой левой ячейки – это бит обратной связи, который равен сумме по модулю 2 битов ячеек S_0, S_1, \dots, S_{n-1} , умноженных на коэффициенты a_1, a_2, \dots, a_n .

Если некоторые из коэффициентов a_1, a_2, \dots, a_n равны нулю, то соответствующие сумматоры по модулю 2 из цепи обратной связи исключают. В моменты времени $t = 0, 1, 2, \dots$ на выходе регистра генерируется последовательность x_0, x_1, x_2, \dots .

Пример 4-хразрядного РСЛОС с коэффициентами $a_1=a_2=0$, $a_3=a_4=1$ и начальным состоянием $(S_0, S_1, S_2, S_3) = (1, 0, 1, 1)$ представлен на рисунке 1.4.3.

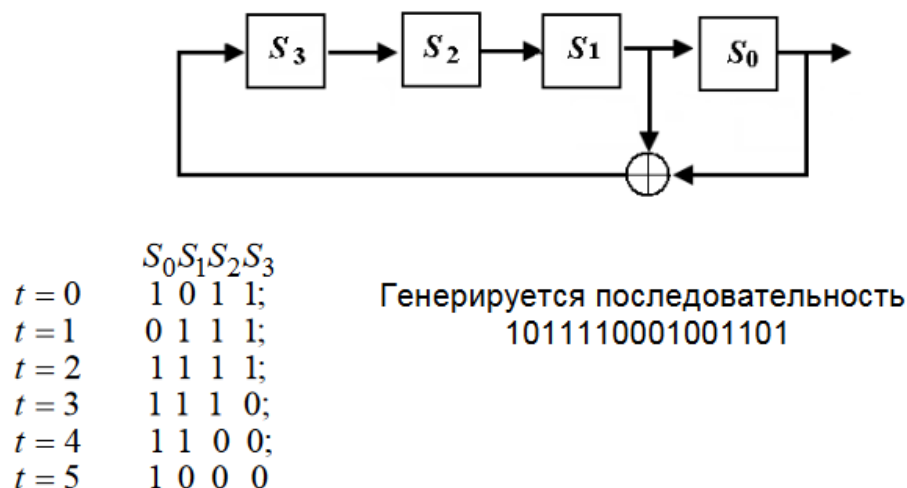


Рисунок 1.4.3 – Пример четырехразрядного регистра сдвига с линейной обратной связью

Если все разряды регистра станут равны нулю, то регистр перестанет менять свое значение и останется нулевым. При этом генерации случайных чисел не будет – все выходные байты будут нулевые. Так происходит потому, что операция XOR от всех '0' также будет равна '0', и при этом обратная связь через XOR не сможет произвести '1', чтобы продолжалось генерирование псевдослучайных чисел.

Чтобы предотвратить такое событие, регистр сдвига предварительно перед началом генерации чисел должен быть обязательно загружен ненулевым значением старта (его называют *вектор начального состояния*). Это значение может быть любым ненулевым числом. Последовательность чисел, которую выдает РСЛОС, напрямую зависит от значения вектора начального состояния. После каждой загрузки вектора начального состояния всегда будет получена одна и та же последовательность псевдослучайных чисел снова и снова, пока не загрузите в качестве вектора начального состояния другое значение. С другим значением последовательность генерируемых псевдослучайных чисел поменяется.

Хорошее значение вектора начального состояния можно получить из текущего времени и/или даты (при наличии в системе часов реального

времени – RTC), а также от значения температуры (при наличии измерения температуры и непостоянного значения температуры).

Вектор начального состояния также можно получить из текстового пароля, складывая по определенному закону его символы. Другой источник вектора начального состояния - аналого-цифровой преобразователь (АЦП), который встроен во многие микроконтроллеры (к примеру, многоканальный АЦП имеется почти во всех моделях AVR). С помощью АЦП можно измерить напряжение питания, некоторое положение какого-нибудь сенсора, или даже усиленное напряжение шума Джонсона (тепловой шум) на диоде Зенера (стабилитрон). Получение из шума случайных чисел - общая практика в прикладной криптографии.

Однако, иногда необходимо использовать в качестве вектора начального состояния строго определенное число, чтобы иметь возможность получить заранее спрогнозированную, однозначно воспроизводимую последовательность псевдослучайных данных. Например, это может потребоваться для получения ключа в XOR-шифровании [6].

РСЛОС, которые генерируют *PN*-последовательности, называются *регистрами максимальной длины*.

Важной характеристикой регистра максимальной длины является *объем ансамбля*. Так называют число различных *PN*-последовательностей для заданного РСЛОС длины *n*.

РСЛОС являются базовым элементом многих потоковых шифров. Это обусловлено:

- высоким быстродействием алгоритмов, построенных на базе РСЛОС;
- применением в регистрах только простых операций: сложения и умножения;
- способностью регистров генерировать последовательности с большим периодом и хорошими статистическими свойствами.

1.5 Исследование свойств последовательностей, генерируемых РСЛОС

Для исследования свойств PN -последовательностей, получаемых, в том числе, в РСЛОС, применяют *набор статистических тестов*. Это совокупность статистических критериев, специализированных для испытания соответствия анализируемой PN -последовательности гипотезе о независимости и равновероятности ее элементов [7].

Любой тест заключается в вычислении по анализируемой последовательности некоторой статистики, имеющей знакомое распределение для настоящей случайной последовательности, и применении критерия согласия.

Стандартными наборами статистических тестов являются набор тестов Д.Кнута, набор тестов NIST (Института стандартов США), пакет TestOut (Л'Эйкуера), пакет DIEHARD (Дж. Марсальи) и другие.

В 2004 году российскими учеными Б.Я.Рябко и А.И.Пестунов был разработан новый статистический тест «Стопка книг» [8]. В работе [9] показана эффективность этого теста в сравнении с тестами NIST.

Генератор, который проходит все статистические тесты набора, называется *статистически безопасным*.

Это означает, что:

- ни один статистический тест не обнаруживает в выходной последовательности генератора (РСЛОС) каких-либо закономерностей;
- каждый бит сгенерированной им последовательности возникает в результате сложного преобразования над всеми начальными битами;
- получив на вход разные начальные биты, генератор выдает на выходе статистически независимые псевдослучайные последовательности.

Примерами статистических (графических) тестов, используемых в данной работе для анализа полученной PN -последовательности, являются следующие:

1. Гистограмма распределения элементов последовательности;
2. Распределение на плоскости;

3. Автокорреляционная функция;
4. Графический спектральный тест

1.5.1 Гистограмма распределения элементов последовательности

Гистограмма распределения элементов последовательности применяется для оценки равномерности генерируемой последовательности и определения частоты построения её символов (по стандартной методике построения гистограмм).

Гистограмма – это графическое представление распределения частот в виде прилегающих друг к другу прямоугольников, основаниями которых служат отрезки, равные ширине классов, а площади прямоугольника пропорциональны частотам в этих классах [10]. Иными словами, это график, аппроксимирующий плотность распределения случайных данных.

При построении гистограммы область значений случайной величины (x_{\min}, x_{\max}) разбивается на некоторое количество сегментов, а затем подсчитывается процент попадания данных в каждый из сегментов.

Построение гистограммы может быть выполнено в программной среде MathCAD при помощи функций:

1) *hist* (*int*, *x*) – возвращает вектор частоты попадания случайной величины *x* в интервалы, определяемые вектором сегментов *int* на отрезке (x_{\min}, x_{\max}) , сегменты находятся в порядке возрастания $x_{\min} < int < x_{\max}$.

Порядок построения гистограммы:

1.1. Получение выборки на основании работы РСЛОС.

1.2. Упорядочение случайной величины. Для этого используется встроенная функция Mathcad: *sort*(*x*) – сортировка выборки *x* в порядке возрастания.

1.3. Группировка выборочных данных *x* по интервалам. Для этого создается массив *int*, размерность которого равна числу интервалов. В массив *int* записываются координаты начала интервалов группировки.

1.4. Определяется количество попадания данных из выборки в каждый

интервал группировки.

1.5. Построение гистограммы

Недостаток функции *hist* состоит в необходимости дополнительного определения массива интервалов построения гистограммы.

2) *histogram (bin, x)* – возвращает двумерную матрицу на отрезке (x_{\min}, x_{\max}) , один столбец которой содержит середины разбиения отрезка на *bin* сегментов, второй – вектор частоты попадания случайной величины *x*.

На рисунке 1.5.1, а представлен пример гистограммы распределения элементов последовательности, в которой есть все возможные члены, а разброс частот символов стремится к нулю. На рисунке 1.5.1, б представлена гистограмма, которая не проходит тест, т.к. чётко прослеживается её распределение.

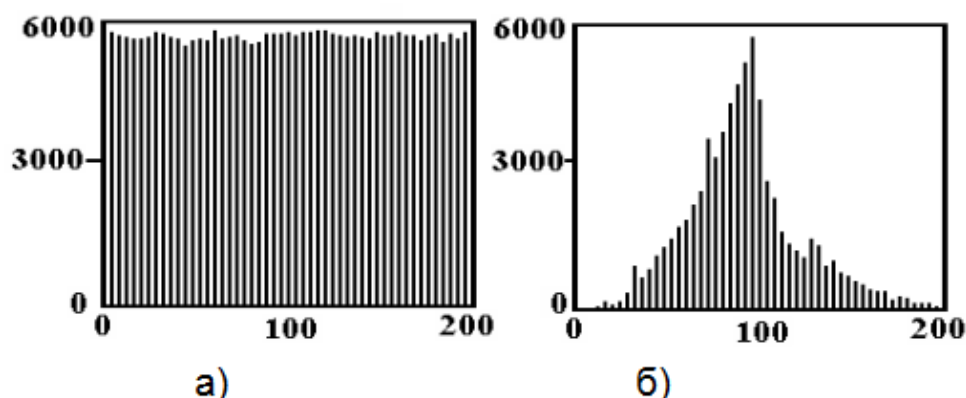


Рисунок 1.5.1 – Пример гистограммы распределения элементов последовательности с минимальным разбросом частот символов (а) и с высоким разбросом частот (б).

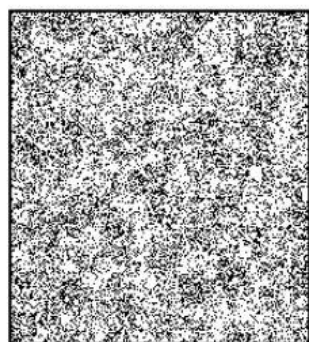
1.5.2 Распределение на плоскости.

Данный тест предназначен для определения зависимостей между элементами исследуемой последовательности [7].

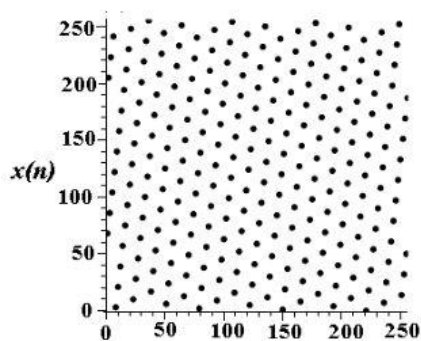
На поле размером $(2^R-1) \times (2^R+1)$, где R – разрядность чисел последовательности, необходимо построить точки с координатами $(x_i; x_{i+1})$, где x_i – члены последовательности; $i = 1, 2, \dots, n$; n – длина последовательности.

Если между элементами последовательности отсутствуют зависимости,

то точки на поле расположены хаотично (рисунок 1.5.2, *а*), а если на поле присутствуют зависимости, наблюдаются «узоры», то последовательность – неслучайна (рисунок 1.5.2, *б*).



а



б

Рисунок 1.5.2 – Пример случайного распределения элементов генерируемой последовательности (*а*) и неслучайного (*б*).

Для последовательностей большой длины хорошим результатом является абсолютно черное поле (рис. 1.5.3)



Рисунок 1.5.3 – Пример распределения на плоскости для случайной последовательности большой длины

1.5.3. Автокорреляционная функция

Автокорреляционная функция применяется для обнаружения корреляции между сдвинутыми копиями исследуемой последовательности.

Данный тест может обнаруживать зависимость между подпоследовательностями анализируемой последовательности.

Для этого члены исследуемой последовательности x_0, x_1, \dots, x_{n-1} представляются в битовом виде, а затем полученную битовую

последовательность изменяют по правилу $1 \rightarrow 1, 0 \rightarrow -1$.

Общий член новой последовательности получается следующим образом:

$$b_i = (-1)^{1-x_i}, i=0,1,2,\dots,n-1.$$

Далее находят всплески корреляции:

$$c_j = \frac{\sum_{i=0}^{n-1} b_i \cdot b_{(i+j) \bmod n}}{\sum_{i=0}^{n-1} b_i^2}, j = 0,1, \dots, n-1. \quad (1.5.1)$$

Для последовательности, близкой к случайной, значения всплесков корреляции стремятся к нулю во всех точках, кроме кратных длине последовательности. В случае наличия большого числа таких всплесков прослеживается зависимость между элементами последовательности.

На рисунке 1.5.4 представлены примеры построения автокорреляционной функции для разных генерируемых последовательностей.

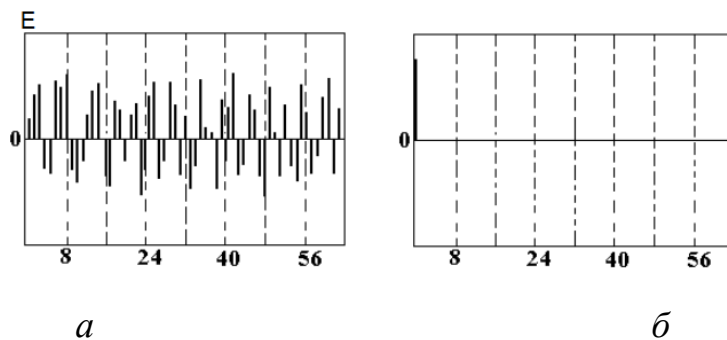


Рисунок 1.5.4 – Пример построения автокорреляционной функции для генерируемой последовательности с зависимыми элементами (а) и независимыми (б)

1.5.4. Графический спектральный тест

Графический спектральный тест позволяет оценить периодические свойства последовательностей на основании анализа высоты выбросов дискретного преобразования Фурье.

Заданная двоичная последовательность длины n преобразуется в другую последовательность по правилу $1 \rightarrow 1$, $0 \rightarrow -1$. К полученной последовательности применяют дискретное преобразование Фурье и получают последовательность гармоник.

Для теста рекомендуется брать не менее 1000 бит последовательности.

У последовательности, чьи свойства близки к свойствам истинно случайной последовательности, число гармоник, чьи длины значительно превышают среднюю длину гармоники, должно стремиться к нулю (рисунок 1.5.5). В противном случае, последовательность не является случайно (рисунок 1.5.6).

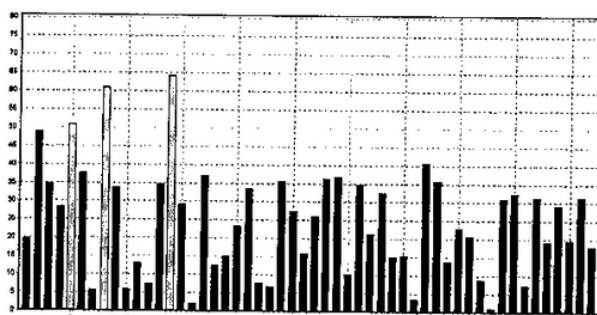


Рисунок 1.5.5 – Пример спектрального графического теста с «положительным» результатом

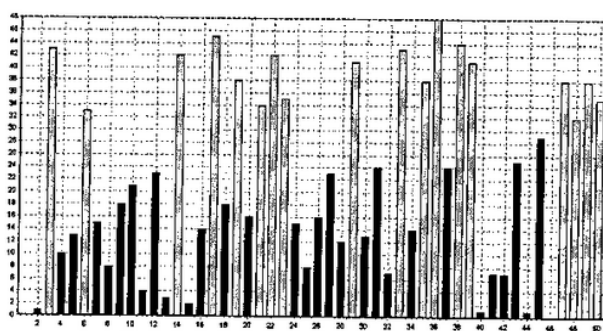


Рисунок 1.5.6 – Пример спектрального графического теста с «отрицательным» результатом

Результаты всех графических тестов интерпретируются человеком, поэтому на их основе выводы могут быть неоднозначными

2. Построение таблицы и схем

2.1 Выбор характеристического (примитивного) полинома, позволяющего минимизировать схемную реализацию регистра

Период регистра сдвига — это минимальная длина получаемой последовательности до начала её повторения. Период генерируемой последовательности максимален и равен 2^n-1 , если многочлен обратной связи является примитивным.

Для этого необходимо выполнение следующих условий:

- четное число отводов;
- номера отводов, взятые все вместе, взаимно просты.

Число всех возможных примитивных многочленов равно $\phi(2^n-1)/n$, где ϕ – функция Эйлера.

Регистр, заданный примитивным многочленом, называется регистром сдвига максимального периода, а генерируемые последовательности – последовательностями максимального периода (*PN*-последовательностями).

Примеры примитивных полиномов представлены в разделе 1.2 настоящей работы.

Для того чтобы минимизировать схемную реализацию регистра сдвига заданной разрядности с обратной связью необходимо, чтобы количество отводов (кол-во слагаемых в полиноме) было минимальным.

Одним из таких примитивных полиномов для 16-разрядного РСЛОС является следующий:

$$x^{16}+x^5+x^3+x^2+1 \quad (2.1)$$

Период данной последовательности равен $2^{16}-1=65535$.

2.2 Разработка функциональной схемы регистра

Функциональная схема для выбранного полинома (2.1) представлена в Приложении А.

Регистр сдвига составлен из 16-ти последовательно включенных триггеров $S_0 \dots S_{15}$ (выход одного подключен ко входу другого), и обратная связь реализована операцией XOR (суммирование по модулю 2) от выбранных разрядов регистра, соответствующих примитивному полиному. Количество элементов XOR на схеме равно трём.

Исходное состояние регистра задается вектором начального состояния $a_0 \dots a_{15}$. Вектор начального состояния определен в разделе 2.3 данной работы.

2.3 Разработка принципиальной электрической схемы и выбор вектора начального состояния

Для построения таблицы генерации PN-последовательности и анализа статистических свойств полученного 16-разрядного РСЛОС данной работой предусмотрена его симуляция в среде Simulink Matlab.

Принципиальная схема 16-разрядного РСЛОС представлена на рисунке Б.1.

Схема РСЛОС построена на базе D-триггеров. В системе Simulink обозначается как D-Latch:

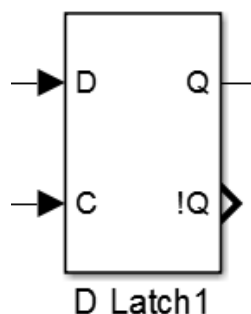


Рисунок 2.3.1 – Внешний вид блока D-триггера в Simulink

Вход D-триггера обозначен символом «D», триггер управляется от синхросигнала, поступающего на вход «C». Выходы D-триггера обозначены

как Q (прямой) и !Q (инверсный).

Синхронизирующий сигнал генерируется блоком Pulse Generator2. Для простоты реализации схемы, вектором начального состояния выбран единичный импульс [1 0 0 0 0 0 0 0 0 0 0 0 0 0 0], который задается блоком Pulse Generator1 и имеет форму единичного прямоугольного импульса (см. рисунок 2.3.2):

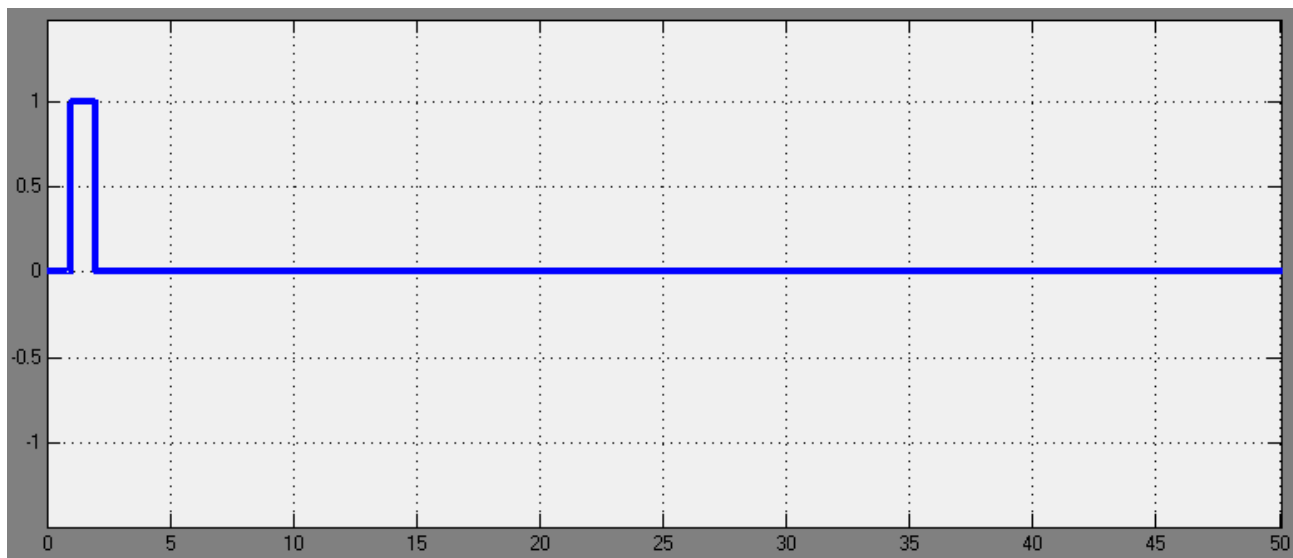


Рисунок 2.3.2 – Вектор начального состояния

2.4 Таблица генерации PN-последовательности. Анализ ее статистических свойств на основе различных свойств

Таблица генерации *PN*-последовательности, полученная путем симуляции схемы в среде Simulink Matlab, представлена в Приложении В.

Из таблицы можно заметить, что сгенерированная *PN*-последовательность начинает повторяться с 65536-го символа, что соответствует периоду последовательности (2.2).

Для оценки статических свойств сгенерированной 16-разрядным РСЛОС *PN*-последовательности выполнен набор статистических тестов, описанный в разделе 1.5 настоящей работы.

2.4.1 Гистограмма распределения элементов последовательности

Для построения гистограммы распределения элементов сгенерированной 16-разрядным РСЛОС последовательности в данной работе применена команда *hist(...)* в программной среде Matlab.

Команда *hist (Y,M)* возвращает вектор чисел попаданий значений элементов вектора *Y* (сгенерированная последовательность) в *M* интервалов с представлением этих чисел в виде столбцовой диаграммы.

На рисунке Г.1 представлена гистограмма распределения сгенерированной последовательности. На полученной гистограмме видим, что разброс частот символов стремится к нулю, так как период сгенерированной последовательности является максимальным. Следовательно, сгенерированная последовательность «успешно» прошла статистический тест методом построения гистограммы.

2.4.2 Распределение на плоскости

На поле размером 65535 x 65535, построим точки с координатами $(x_i; x_{i+1})$, где x_i – члены последовательности; $i = 1, 2, \dots, 65535$; n – длина последовательности. Для построения используем встроенную функцию в программной среде Matlab – *Scatter()*.

На рисунке Д.1 представлено распределение значений сгенерированной последовательности на плоскости. На полученном распределении видим, что, точки на поле расположены хаотично, «узоры» не наблюдаются, то поле практически полностью закрашено. Следовательно, между элементами последовательности отсутствуют зависимости. Сгенерированная последовательность «успешно» прошла статистический тест методом построения распределения на плоскости.

2.4.3 Автокорреляционная функция

Для построения графика автокорреляционной функции применяется базовый блок в среде моделирования Simulink – *Auto Correlator* (см. рисунок 2.4.1).



Рисунок 2.4.1 – Внешний вид блока *Auto Correlator* в Simulink

Внутри данного блока задается параметр размера буфера *Length of bugger* - должен быть равен периоду генерируемой последовательности 65535.

На рисунке Е.1 представлен полученный график автокорреляционной функции сгенерированной последовательности. На графике можем наблюдать малое количество всплесков (по центру и по краям), следовательно, зависимость между элементами последовательности не прослеживается. Сгенерированная последовательность «успешно» прошла статистический тест методом построения автокорреляционной функции.

2.4.3 Графический спектральный тест

Для спектрального анализа генерируемой последовательности применяется базовый блок в среде моделирования Simulink – *Spectrum Analyzer* (см. рисунок 2.4.3).



Рисунок 2.4.3 – Внешний вид блока *Spectrum Analyzer* в Simulink

На рисунке Ж.1 представлен полученный график дискретного преобразования Фурье для сгенерированной последовательности. У последовательности число гармоник, чьи длины значительно превышают среднюю длину гармоник, стремится к нулю, следовательно, последовательность можно назвать случайной. Сгенерированная последовательность «успешно» прошла графический спектральный тест.

3. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

3.1 Организация и планирование работ

Наглядным результатом планирования работ является линейный график реализации проекта. Группа участников состоит из инженера (И), а также научный руководитель (НР). Для выполнения научного исследования сформирован ряд работ, назначены должности исполнителя для каждого этапа работы Таблице 3.1.1.

Таблица 3.1.1 - Перечень работ и продолжительность их выполнения

Этапы работы	Исполнители	Загрузка исполнителей
Постановка целей и задач, получение исходных данных	НР	НР – 100%
Составление и утверждение ТЗ	НР, И	НР – 100% И – 10%
Подбор и изучение материалов по тематике	НР, И	НР – 30% И – 100%
Разработка календарного плана	НР, И	НР – 100% И – 10%
Обсуждение литературы	НР, И	НР – 30% И – 100%
Выбор структурной схемы устройства	НР, И	НР – 100% ИП – 70%
Выбор функциональной схемы устройства	НР, И	НР – 100% И – 80%
Расчет функциональной схемы устройства	И	И – 100%
Выбор схемы внешних проводок	НР, И	НР – 100% И – 80%
Расчет схемы внешних проводок	И	И – 100%
Оформление расчетно-пояснительной записки	И	И – 100%
Оформление графического материала	И	И – 100%
Подведение итогов	НР, И	НР – 60% И – 100%

3.1.1 Продолжительность этапов работ

Расчет продолжительности этапов работ будем производить с помощью опытно-статического метода, который реализуется двумя способами:

- аналоговый;
- экспертный.

Аналоговый метод – не подходит, так как, требует не устаревшего аналога проекта.

Экспертный способ используется при отсутствии вышеуказанных информационных ресурсов и предполагает генерацию необходимых количественных оценок специалистами конкретной предметной области, опирающимися на их профессиональный опыт и эрудицию. Будем использовать этот метод. Для определения вероятных (ожидаемых) значений продолжительности работ $t_{ож}$ применяется следующая формула:

$$t_{ож} = \frac{3 \cdot t_{min} + 2 \cdot t_{max}}{5} \quad (3.1.1)$$

где t_{min} – минимальная продолжительность работы, дн.;

t_{max} – максимальная продолжительность работы, дн.;

Для выполнения перечисленных в таблице 3.1.1 работ требуются специалисты:

- инженер – в его роли действует исполнитель НИР (ВКР);
- научный руководитель.

Для построения линейного графика необходимо рассчитать длительность этапов в рабочих днях, а затем перевести ее в календарные дни. Расчет продолжительности выполнения каждого этапа в рабочих днях ($T_{РД}$) ведется по формуле:

$$T_{РД} = \frac{t_{ож}}{K_{ВН}} \cdot K_{Д} \quad (3.1.2)$$

где $t_{ож}$ – продолжительность работы, дн.;

$K_{ВН}$ – коэффициент выполнения работ, учитывающий влияние внешних факторов на соблюдение предварительно определенных длительностей, в

частности, возможно $K_{\text{вн}} = 1$;

$K_{\text{д}}$ – коэффициент, учитывающий дополнительное время на компенсацию непредвиденных задержек и согласование работ ($K_{\text{д}} = 1\text{--}1,2$; в этих границах конкретное значение принимает сам исполнитель).

Расчет продолжительности этапа в календарных днях ведется по формуле:

$$T_{\text{кд}} = T_{\text{рд}} \cdot T_{\text{к}} \quad (3.1.3)$$

где $T_{\text{кд}}$ – продолжительность выполнения этапа в календарных днях;



















$T_{\text{к}}$ – коэффициент календарности, позволяющий перейти от длительности работ в рабочих днях к их аналогам в календарных днях, $T_{\text{к}} = 1,205$.

Определение продолжительности этапов работ и их трудоемкости по исполнителям, занятым на каждом этапе приведено в таблице 3.1.2

Таблица 3.1.2 – Трудозатраты на выполнение проекта

Этап	Исполнители	Продолжительность работ, дни			Трудоемкость работ по исполнителям чел.- дн.			
					$T_{РД}$		$T_{КД}$	
		t_{min}	t_{max}	$t_{ож}$	НР	И	НР	И
1	2	3	4	5	6	7	8	9
Постановка задачи	НР	3	5	3,1	3,10	–	3,8	–
Разработка и утверждение технического задания (ТЗ)	НР, И	2	4	2,9	3,09	0,5	3,44	0,40
Подбор и изучение материалов по тематике	НР, И	13	16	13,7	4,36	14,52	5,30	17,75
Разработка календарного плана	НР, И	2	3	2,4	2,64	0,26	3,18	0,32
Обсуждение литературы	НР, И	2	5	3,2	1,06	3,52	1,27	4,24
Разработка функциональной схемы регистра.	НР, И	6	13	8,1	8,85	6	10,54	7,65
Разработка схема цифровой логики.	НР, И	7	10	7,8	8,31	6,55	9,74	7,81
Разработка принципиальной электрической схемы и выбор вектора начального состояния.	И	9	15	12,6	–	11,90	–	14,82
Построение таблицы генерации PN-последовательности. Анализ ее статистических свойств на основе различных тестов.	НР, И	4	10	6,4	7,04	5,63	8,46	6,77
Оформление графического материала	И	6	6	5,5	–	6,3	–	7,25
Подведение итогов	НР, И	4	6	5,1	3,4	5,86	4,44	7,89
Итого:				70,8	42,09	61,04	50,17	74,9

Таблица 3.1.3 – Линейный график работ

Этап	НР	И	Март			Апрель			Май			Июнь	
			10	20	30	40	50	60	70	80	90	100	110
1	3,8	–											
2	3,44	0,40	 										
3	5,30	17,75											
4	3,18	0,32											
5	1,27	4,24				 							
6	10,54	7,65				 							
7	9,74	7,81					 						
8	–	14,82											
9	8,46	6,77							 				
10	–	7,25											
11	4,44	7,89										 	

НР –  И – 

3.2 Расчет сметы затрат на выполнение проекта

В состав затрат на создание автоматизированной системы дозирования сырья включается величина всех расходов, необходимых для реализации комплекса работ, составляющих содержание данной разработки. Расчет сметной стоимости ее выполнения производится по следующим статьям затрат:

- материалы и покупные изделия;
- заработная плата;
- социальный налог;
- расходы на электроэнергию (без освещения);
- амортизационные отчисления;
- командировочные расходы;
- оплата услуг связи;
- арендная плата за пользование имуществом;
- прочие услуги (сторонних организаций);
- прочие (накладные расходы) расходы.

3.2.1 Расчет затрат на материалы

Далее в таблице приведена стоимость основного оборудования, а также других материальных ценностей, расходуемых непосредственно на разработку системы дозирования сырья.

Таблица 3.2.4 – Расчет затрат на материалы

Наименование материалов	Цена за ед., руб.	Кол-во	Сумма, руб.
Бумага для принтера формата А4	250	1 шт.	250
Картридж для принтера	1600	1 шт.	1600
Лицензия ПО MATLAB	2150	1 шт.	2150
Итого:			4000

Также рассчитываются транспортно-заготовительные расходы (ТЗР),

связанные с транспортировкой от поставщика к потребителю, хранением и прочими процессами, обеспечивающими движение (доставку) материальных ресурсов от поставщиков к потребителю. Сюда же включаются расходы на совершение сделки купли-продажи (т.н. транзакции). Приблизительно они оцениваются в процентах к отпускной цене закупаемых материалов, как правило, это $5 \div 20 \%$.

Допускаем, что $TЗР = 5\%$, от отпускной цены материалов, тогда расходы на материалы с учетом $TЗР$ равны $C_{\text{мат}} = 4000 * 1,05 = 4200$ руб.

3.2.2 Расчет заработной платы

Для расчета расходов на заработную плату, принимаются заработная плата научного руководителя и исполнителя, а также премии, входящие в фонд заработной платы.

Среднедневная тарифная заработная плата (при шести дневной рабочей неделе) ($ЗП_{\text{дн-т}}$) рассчитывается по формуле:

$$ЗП_{\text{дн-т}} = MO/25,083 \quad (3.2.4)$$

Для пятидневной рабочей недели в месяце в среднем 21,083 рабочих дня, поэтому среднедневная тарифная заработная плата для инженера рассчитывается по формуле:

$$ЗП_{\text{дн-т}} = MO/21,083 \quad (3.2.5)$$

Пример расчета затрат на полную заработную плату приведены в таблице 3.2.6. Затраты времени, по каждому исполнителю в рабочих днях с округлением до целого взяты из таблицы 3.1.2. Для учета в ее составе премий, дополнительной зарплаты и районной надбавки используется следующий ряд коэффициентов: $K_{\text{ПР}} = 1,1$; $K_{\text{доп.ЗП}} = 1,188$; $K_{\text{р}} = 1,3$. Таким образом, для перехода от тарифной (базовой) суммы заработка исполнителя, связанной с участием в проекте, к соответствующему полному заработку (зарплатной части сметы) необходимо первую умножить на интегральный коэффициент $K_{\text{и}} = 1,1 * 1,188 * 1,3 = 1,699$. Вышеуказанное значение $K_{\text{доп.ЗП}}$ применяется при шестидневной рабочей неделе, при пятидневной оно равно 1,113, соответственно в этом случае $K_{\text{и}} = 1,62$.

Таблица 3.2.6 – Затраты на заработную плату

Исполнитель	Оклад, руб./мес.	Среднедневная ставка, руб./раб. день	Затраты времени, раб. дни	Коэффициент	Фонд з/платы, руб.
НР	33664	1342.09	42	1,699	95 768,8
И	15470	733,77	61	1,62	72 511,15
Итого:					168 279,95

3.2.3 Расчет затрат на социальный налог

Затраты на единый социальный налог (ЕСН), включающий в себя отчисления в пенсионный фонд, на социальное и медицинское страхование, составляют 30 % от полной заработной платы по проекту, т.е. $C_{\text{соц.}} = C_{\text{зп}} * 0,3$.
Итак, в нашем случае $C_{\text{соц.}} = 168\,279,95 * 0,3 = 50\,483,98$ рубля.

3.2.4 Расчет затрат на электроэнергию

Затраты на электроэнергию, потраченную в ходе выполнения проекта на работу используемого оборудования, рассчитываются по формуле:

$$C_{\text{эл.об.}} = P_{\text{об}} \cdot t_{\text{об}} \cdot Ц_{\text{э}} \quad (3.2.6)$$

где $P_{\text{об}}$ – мощность, потребляемая оборудованием, кВт;

$Ц_{\text{э}}$ – тариф на 1 кВт·час;

$t_{\text{об}}$ – время работы оборудования, час.

Тариф на 1 кВт·час (для ТПУ $Ц_{\text{э}} = 6,59$ руб./кВт·час)

Время работы оборудования вычисляется на основе итоговых данных таблицы 3.1.2 для инженера ($T_{\text{рд}}$) из расчета, что продолжительность рабочего дня равна 8 часов.

$$t_{\text{об}} = T_{\text{рд}} * K_{\text{т}}, \quad (3.2.7)$$

Мощность, потребляемая оборудованием, определяется по формуле:

$$P_{\text{об}} = P_{\text{ном.}} * K_{\text{с}} \quad (3.2.8)$$

где $P_{\text{ном.}}$ – номинальная мощность оборудования, кВт;

$K_{\text{с}} \leq 1$ – коэффициент загрузки, зависящий от средней степени

использования номинальной мощности. Для технологического оборудования малой мощности $K_C = 1$.

Пример расчета затраты на электроэнергию для технологических целей приведен в таблице 3.2.7

Таблица 3.2.7 – Затраты на электрическую энергию технологическую

Наименование оборудования	Время работы оборудования t_{OB} , час	Потребляемая мощность P_{OB} , кВт	Затраты Δ_{OB} , руб.
Персональный компьютер	491,2*0,6	0,4	776,9
Лазерный Принтер	2*0,3	0,3	1,2
Итого:			778,1

3.2.5 Расчет амортизационных расходов

Амортизация используемого оборудования за время выполнения проекта рассчитывается по формуле:

$$C_{AM} = \frac{N_A * C_{OB} * t_{pf} * n}{F_d}, \quad (3.2.9)$$

где N_A – годовая норма амортизации единицы оборудования;

C_{OB} – балансовая стоимость единицы оборудования с учетом ТЗР. При невозможности получить соответствующие данные из бухгалтерии она может быть заменена действующей ценой, содержащейся в ценниках, прейскурантах и т.п.;

F_d – действительный годовой фонд времени работы соответствующего оборудования, берется из специальных справочников или фактического режима его использования в текущем календарном году.

t_{pf} – фактическое время работы оборудования в ходе выполнения проекта, учитывается исполнителем проекта;

n – число задействованных однотипных единиц оборудования.

При использовании нескольких типов оборудования расчет по формуле

делается соответствующее число раз, затем результаты суммируются.

Рассчитаем амортизацию для ПК. В соответствии с постановлением правительства Российской Федерации «О классификации основных средств, включенных в амортизационные группы» персональный компьютер, относится ко второй амортизационной группе основных средств, срок полезного использования варьируется от 2 до 3 лет. Необходимо задать конкретное значение срока амортизации (СА), пусть это будет 2,6. Далее определяется N_A как величина обратная СА, в данном случае это $1 : 2,6 = 0,38$.

Рассчитаем F_d для ПК. В 2020 г. (302 рабочих дней при шестидневной рабочей неделе) можно принять $F_d = 302 * 8 = 2416$ часов;

Стоимость ПК 45000 руб.; время использования 491,2 часа, тогда для него $C_{AM} = (0,38 * 45000 * 491,2 * 1) / 2416 = 3476,6$ руб.

Рассчитаем амортизацию для принтера. $F_d = 500$ часов; стоимость принтера 10700 руб.; время пользования 40 часов.; $N_A = 1 : 2,5 = 0,4$ (срок полезного использования от 2 до 3 лет), тогда его $C_{AM} = (0,4 * 10700 * 2 * 1) / 500 = 17,12$ руб.

Итого начислено амортизации 3493,74 руб.

3.2.6 Расчет расходов, учитываемых непосредственно на основе платежных (расчетных) документов (кроме суточных)

Сюда относятся:

- командировочные расходы, в т.ч. расходы по оплате суточных, транспортные расходы, компенсация стоимости жилья;
- арендная плата за пользование имуществом;
- оплата услуг связи;
- услуги сторонних организаций.
- Норма оплаты суточных – 100 руб./день

Время пребывания в командировке составило – 47 календарных дня (с учетом дней приезда и отъезда); оплата проживания в общежитии – 50

руб./день*47 дня = 2350 руб; оплата проезда в обе стороны (автомобиль) – 1900руб.; услуги связи – 740 руб.;

Итого $C_{нр} = (47 - 1) * 100 + 2350 + 1900 + 740 = 9590$ рублей.

3.2.7 Расчет прочих расходов

Прочие расходы отражают расходы на выполнение проекта, которые не учтены в предыдущих статьях, их следует принять равными 10% от суммы всех предыдущих расходов, показано в формуле ниже:

$$C_{\text{проч.}} = (C_{\text{мат}} + C_{\text{зп}} + C_{\text{соц}} + C_{\text{эл.об.}} + C_{\text{ам}} + C_{\text{нр}}) \cdot 0,1 \quad (3.2.10)$$

Таким образом:

$$C_{\text{проч.}} = (4200 + 168\,279,95 + 50\,483,98 + 778,1 + 3493,74 + 9590) \cdot 0,1 = 23\,682,6 \text{ рублей.}$$

3.2.8 Расчет общей себестоимости разработки

Проведя расчет по всем статьям сметы затрат на разработку, можно определить общую себестоимость проекта. Смета на затраты приведены ниже в таблице 3.2.8

Таблица 3.2.8 – Смета затрат на разработку проекта

Статья затрат	Условное обозначение	Сумма, руб.
Материалы и покупные изделия	$C_{\text{мат}}$	4200
Основная заработная плата	$C_{\text{зп}}$	168 279,95
Отчисления в социальные фонды	$C_{\text{соц}}$	50 483,98
Расходы на электроэнергию	$C_{\text{эл.}}$	778,1
Амортизационные отчисления	$C_{\text{ам}}$	3493,74
Непосредственно учитываемые расходы	$C_{\text{нр}}$	9590
Прочие расходы	$C_{\text{проч}}$	23 682,6
Итого:		260 508,4

Таким образом, затраты на разработку составили $C = 260\,508,4$ рублей.

3.2.9 Расчет прибыли

Прибыль от реализации проекта в зависимости от конкретной ситуации (масштаб и характер получаемого результата, степень его определенности и коммерциализации, специфика целевого сегмента рынка и т.д.) может определяться различными способами. Без применения сложных методов расчета, прибыль следует принять в размере $5 \div 20 \%$ от полной себестоимости проекта. В данном случае она составляет 39 076,3 рубля, (15 %) от расходов на разработку проекта.

3.2.10 Расчет НДС

НДС составляет 20% от суммы затрат на разработку и прибыли. В нашем случае это $(260\,508,4 + 39\,076,3) * 0,2 = 299\,584,7 * 0,2 = 59\,916,94$

3.2.11 Цена разработки НИР

Цена равна сумме полной себестоимости, прибыли и НДС, в нашем случае $C_{\text{НИР(КР)}} = 260\,508,4 + 39\,076,3 + 59\,916,94 = 359\,501,64$ рубля.

3.3 Оценка экономической эффективности проекта

Эффективность проекта обусловлена, в первую очередь, заменой устаревшего оборудования или отдельных его частей на более высокотехнологичное, что несомненно должно привести к более длительной эксплуатации оборудования при его более высокой отказоустойчивости и соответственно экономии в затратах на его ремонт. Нельзя дать конкретную количественную оценку экономической эффективности, так как отсутствуют точные данные об объекте управления и условиях его эксплуатации.

В данной главе была рассчитана смета затрат на выполнение проекта. В результате данных расчетов получили стоимость НИР равную 359 501,64 рублей.

4. Социальная ответственность

Введение к разделу

Объектом исследования является двоичный регистр сдвига с линейной обратной связью. За последнее десятилетие существенно изменились состав и структура технических средств, применяемых в автоматизированных системах управления технологическими процессами (АСУТП). Современные АСУТП создаются на основе локальных вычислительных сетей и нового поколения микропроцессорных контроллеров с широким спектром функциональных возможностей. Основными чертами технического обеспечения современных АСУТП являются: – сохранение результатов измерения технологических параметров за любой период времени и вывод информации в удобном для оператора виде на экран мониторов операторских станций; – мнемосхемы технологических процессов любой степени детализации с указанием текущих значений технологических параметров и сигнализацией состояния оборудования, выводимые на экран мониторов операторских станций.

С каждым годом возрастает интенсивность применения компьютерной техники в сферах жизнедеятельности человека. При работе с компьютером человек подвергается воздействию ряда опасных и вредных производственных факторов:

- электромагнитных полей;
- радиочастотному, инфракрасному и ионизирующему излучению;
- шуму и вибрации;
- статическому электричеству.

Работа с компьютером характеризуется значительным умственным напряжением, высокой напряженностью зрительной работы и большой нагрузкой на кисти рук при работе с периферийными устройствами ЭВМ.

В рамках выпускной квалификационной работы проводится исследование однородных линейных рекуррентных последовательностей над бинарным полем. Построение последовательностей максимальной длины при помощи регистров сдвига с линейной обратной связью.

4.1. Правовые и организационные вопросы обеспечения безопасности

Оператор АРМ проводит рабочий день в сидячем положении за компьютером. Для сидячей работы за ПК согласно ГОСТ 12.2.032-78 [13] необходимо соблюдение следующих условий:

- высота рабочей поверхности при организации рабочего места женщин и мужчин должна составлять 655 мм;
- высота сиденья для женщин и мужчин должна составлять 420 мм;
- ширина пространства для ног не менее 500 мм;
- высота пространства для ног не менее 600 мм;
- расстояние от сиденья до нижнего края рабочей поверхности не менее 150 мм.

Также необходимо соблюдение следующих требований для подставки для ног [13]:

- подставка для ног должна быть регулируемой по высоте;
- ширина подставки должна быть не менее 300 мм;
- длина подставки должна быть не менее 400 мм;
- поверхность подставки должна быть рифленой;
- по переднему краю подставки следует предусматривать бортик высотой 10 мм.

Согласно ГОСТ 22269-76 [14] необходимо соблюдение следующих правил расположения органов управления

- органы управления должны располагаться в зоне досягаемости моторного поля;
- наиболее важные и часто используемые органы управления должны быть расположены в зоне легкой досягаемости моторного поля;
- органы управления, связанные с определенной последовательностью действий оператора, должны группироваться таким образом, чтобы действия оператора осуществлялись слева направо и сверху вниз;
- расположение функционально идентичных органов управления должно быть единообразным на всех панелях рабочего места;

- расположение органов управления должно обеспечивать равномерность нагрузки обеих рук и ног человека-оператора.

Органы управления, применяемые только для технического обслуживания и регулировки, должны размещаться отдельно от остальных органов управления или быть изолированными от человека-оператора на период выполнения им основной работы.

Органы управления, применяемые только для технического обслуживания и регулировки, должны размещаться отдельно от остальных органов управления или быть изолированными от человека-оператора на период выполнения им основной работы [14].

Согласно ГОСТ 12.2.032-78 [13], необходимо соблюдать следующие требования к размещению средств отображения информации:

- очень часто используемые средства отображения информации, требующие точного и быстрого считывания показаний, следует располагать в вертикальной плоскости под углом $\pm 15^\circ$ от нормальной линии взгляда и в горизонтальной плоскости под углом $\pm 15^\circ$ от сагиттальной плоскости;
- часто используемые средства отображения информации, требующие менее точного и быстрого считывания показаний, допускается располагать в вертикальной плоскости под углом $\pm 30^\circ$ от нормальной линии взгляда и в горизонтальной плоскости под углом $\pm 30^\circ$ от сагиттальной плоскости;
- редко используемые средства отображения информации допускается располагать в вертикальной плоскости под углом $\pm 60^\circ$ от нормальной линии взгляда и в горизонтальной плоскости под углом $\pm 60^\circ$ от сагиттальной плоскости (при движении глаз и повороте головы).

Согласно ГОСТ 21889-76 [15], существуют следующие общие эргономические требования к креслу человека-оператора:

- кресло должно обеспечивать длительное поддержание основной рабочей позы в процессе трудовой деятельности;
- при невозможности покинуть рабочее место длительное время конструкция кресла должна обеспечивать условия для отдыха человека

оператора в кресле;

- кресло оператора должно включать следующие основные элементы: сиденье, спинку и подлокотники. В конструкцию кресла могут быть включены также дополнительные элементы, не обязательные для установки, – подголовник и подставка для ног;

- в конструкции кресла должны регулироваться высота поверхности сиденья и угол наклона спинки. При необходимости должны регулироваться также следующие параметры: высота спинки, высота подлокотников, угол наклона подлокотников, высота подголовника, высота подставки для ног, угол наклона подставки для ног.

Согласно ГОСТ 21958-76 [16], существуют следующие требования к расположению рабочих мест операторов: в залах и кабинах рабочие места операторов необходимо располагать в зоне наилучшего видения информационного поля, которая должна обеспечить однозначное восприятие знаковой индикации.

Согласно [17] каждый работник имеет право на:

- рабочее место, соответствующее требованиям охраны труда;
- обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний в соответствии с федеральным законом;

- отказ от выполнения работ в случае возникновения опасности для его жизни и здоровья вследствие нарушения требований охраны труда, за исключением случаев, предусмотренных федеральными законами, до устранения такой опасности;

- обучение безопасным методам и приемам труда за счет средств работодателя;

- обращение в органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления, к работодателю, в объединения работодателей, а также в профессиональные союзы, их объединения и иные уполномоченные

работниками представительные органы по вопросам охраны труда;

- внеочередной медицинский осмотр в соответствии с медицинскими рекомендациями с сохранением за ним места работы (должности) и среднего заработка во время прохождения указанного медицинского осмотра.

4.2. Производственная безопасность

Проанализируем вредные и опасные факторы, которые могут возникать при разработке, изготовлении и эксплуатации проектируемого решения. Перечень опасных и вредных факторов представлен в Таблица 4.2.1.

Таблица 4.2.1 – Возможные опасные и вредные факторы

Факторы (ГОСТ 12.0.003-2015)	Этапы работ			Нормативные документы
	Разработка	Изготовление	Эксплуатация	
Уровень шума на рабочем месте	+	+	+	СанПиН 2.2.4.3359-16 [9] ГОСТ 12.1.029-80 [10]
Электрический ток	+	+	+	ГОСТ 12.1.038-82 [11]
Уровень электромагнитных излучений	+	+	+	ГОСТ 12.1.002-84 [12] СанПиН 2.2.2/2.4.1340-03 [13]
Микроклимат воздуха рабочей зоны	+	+	+	СанПиН 2.2.4.548-96 [14] СНиП 41-01-2003 [15]
Освещенность рабочей зоны	+	+	+	СП 52.13330.2016 [16]

4.2.1. Уровень шума на рабочем месте

При выполнении работ, специалист может оказаться в зоне повышенного уровня шума, источником которого является оборудование, находящееся в рабочем помещении: персональные компьютеры, устройства печати и поддержки микроклимата (кондиционеры, вентиляция), а также оборудование, которое находится непосредственно в цеху, но производят высокий уровень шума.

Работа, выполняемая оператором за компьютером, оценивается как работа, выполняемая с часто получаемыми указаниями и акустическими сигналами; работа, требующая постоянного слухового контроля; операторская работа по точному графику с инструкцией; диспетчерская работа, и, следовательно, согласно санитарным нормам [18] уровень звука в рабочем помещении не должен превышать 80 дБА. В качестве мер по снижению шума согласно ГОСТ 12.1.029-80 [19] применяют:

- подавление шума в источниках;
- звукоизоляция и звукопоглощение;
- увеличение расстояния от источника шума;
- проверка технического состояния и ремонт системного блока и принтера;
- рациональный режим труда и отдыха.

4.2.2. Электрический ток

Помещение, где расположены персональные вычислительные машины, относится к помещениям без повышенной опасности. Опасное и вредное воздействия на людей электрического тока и электрической дуги проявляются в виде электротравм и профессиональных заболеваний. К мероприятиям по предотвращению возможности поражения электрическим током следует отнести:

- при производстве монтажных работ необходимо использовать только исправный инструмент, аттестованный службой КИПиА;

- с целью защиты от поражения электрическим током, возникающим между корпусом приборов и инструментом при пробое сетевого напряжения на корпус, корпуса приборов и инструментов должны быть заземлены;
- при включенном сетевом напряжении работы на задней панели должны быть запрещены;
- все работы по устранению неисправностей должен производить квалифицированный персонал;
- постоянный контроль за состоянием электропроводки.

Перед началом работы следует убедиться в отсутствии свешивающихся со стола или висящих под столом проводов электропитания, в целостности вилки и провода электропитания, в отсутствии видимых повреждений аппаратуры и рабочей мебели, в отсутствии повреждений и наличии заземления приэкранного фильтра.

Токи статического электричества, наведенные в процессе работы компьютера на корпусах монитора, системного блока и клавиатуры, могут приводить к разрядам при прикосновении к этим элементам. В [20] приведена информация о предельно допустимых значениях напряжений прикосновения и токов. В большинстве случаев разряды при прикосновении к корпусу монитора, системного блока и клавиатуры опасности для человека не представляют, но могут привести к выходу из строя компьютера. Для снижения величин токов статического электричества используются нейтрализаторы, местное и общее увлажнение воздуха, использование покрытия полов с антистатической пропиткой.

4.2.3. Уровень электромагнитных излучений

Рабочее место оператора подвержено влиянию электромагнитных полей (ЭМП). Источниками ЭМП является оборудование, в частности компьютеры (ЭВМ). Большая часть электромагнитного излучения, создаваемого ЭВМ, происходит от видеокабеля и системного блока. В составе современных персональных компьютеров практически все электромагнитное излучение идет

от системного блока. Современные компьютеры выпускаются производителями со специальной металлической защитой внутри системного блока для уменьшения фона электромагнитного излучения. Электромагнитное поле обладает способностью биологического, специфического теплового воздействия на организм человека. При воздействии полей, имеющих напряженность выше предельно допустимого уровня, развиваются нарушения со стороны нервной, сердечно-сосудистой систем, органов пищеварения и некоторых биологических показателей крови.

Степень воздействия электромагнитных излучений на организм человека зависит от диапазона частот, интенсивности воздействия соответствующего фактора, продолжительности облучения, характера излучения, режима облучения, размеров облучаемой поверхности тела и индивидуальных особенностей организма человека.

Критерием безопасности для человека, находящегося в электрическом поле промышленной частоты, принята напряжённость этого поля. Гигиенические нормы для персонала, который систематически находится в этой зоне, установлены согласно [21].

Нормы допустимых уровней напряженности электрических полей зависят от времени пребывания человека в контролируемой зоне. Время допустимого пребывания в рабочей зоне в часах составляет $T=50E-2$. Работа в условиях облучения электрическим полем с напряженностью 20–25 кВ/м продолжается не более 10 минут. При напряженности не выше 5 кВ/м присутствие людей в рабочей зоне разрешается в течение 8 часов [22].

Использование современной офисной техники позволяет избежать повышенных электромагнитных и электрических полей. Возможные способы защиты от ЭМП на путях распространения:

- применение поглотителей мощности;
- увеличение расстояния от источника излучения;
- уменьшение времени пребывания в поле и под воздействием излучения;

- подъем излучателей и диаграмм направленности излучения;
- блокировочные излучения;
- экранирование излучений.

4.2.4. Микроклимат воздуха рабочей зоны

Мероприятия по доведению микроклиматических показателей до нормативных значений включаются в комплексные планы организаций. Для создания благоприятных условий работы, соответствующих физиологическим потребностям человеческого организма, санитарные нормы устанавливают оптимальные и допустимые метеорологические условия в рабочей зоне помещения, выдержки приведены в Таблица 4.2.2 и Таблица 4.2.3 [23].

Таблица 4.2.2 – Оптимальные величины показателей микроклимата

	Период года	
	Холодный	Теплый
Температура воздуха, °С	21-23	23-25
Температура поверхностей, °С	20-24	22-26
Относительная влажность, %	60-40	60-40
Скорость движения воздуха, м/с	0,1	0,1

Таблица 4.2.3 – Допустимые величины показателей микроклимата

Период года	Холодный	Теплый
Температура воздуха, °С:		
• диапазон ниже оптимальных величин	19,0-20,9	20,0-21,9
• диапазон выше оптимальных величин	23,1-24,0	24,1-28,0
Температура поверхностей, °С	18,0-25,0	19,0-29,0
Относительная влажность воздуха, %	15-75	15-75

Скорость движения воздуха, м/с:		
• для диапазона ниже оптимальных величин	0,1 0,2	0,1 0,3
• для диапазона выше оптимальных величин		

В данном случае температура воздуха и температура поверхностей составляют 22 °С и 21 °С при относительной влажности 45 % в холодный период года и 24 °С и 23 °С при относительной влажности воздуха 50 % в теплый период года, что соответствует нормам [24].

4.2.5. Освещенность рабочей зоны

Для безопасной работы человека необходимо, чтобы в помещении присутствовало как естественное освещение, так и искусственное. Для искусственного освещения применяют люминесцентные лампы типа ЛБ. В соответствии с [25] норма освещенности в кабинете должна быть $E_n = 200$ лк. Пульсация при работе с ноутбуком не должна превышать 5% по [22]. Увеличение коэффициента данного параметра снижает зрительную работоспособность, повышает утомляемость, негативно воздействует на нервные элементы головного мозга, а также фоторецепторные элементы сетчатки глаз. Для снижения пульсации лучше использовать светильники, в которых лампы работают от переменного тока частотой 400 Гц и выше.

4.3. Электрический ток

В помещении, где происходит выполнение работы, находится ЭВМ с напряжением питания 220 В. В целом, помещение сухое, непыльное, с нормальной температурой воздуха и поэтому относится к классу помещений без повышенной опасности: переключатели, кнопки и разъемы, клавиатура изолированы, пол покрыт электроизоляционным покрытием. Корпус ЭВМ изготовлен из металлического листа, обладает высокой механической прочностью и высокими экранирующими свойствами, покрыт токонепроводящими полимерными пластмассами. Компьютер подключен к

заземляющему контуру [26].

Электрические изделия по способу защиты человека от поражения электрическим током подразделяются на пять классов: 0, 01, 1, 2, 3.

ЭВМ можно отнести к классу 01, то есть, к изделиям, имеющим рабочую изоляцию, элемент для заземления и провод без заземляющей жилы для присоединения к источнику питания. При начале работы с ЭВМ необходимо проверить герметичность корпуса, не открыты ли токоведущие части. Убедиться в подключении заземляющего проводника к общей шине заземления, проверить его целостность. Если заземляющий проводник отключен, подключать его можно только при отключении машины от питающей сети. Для повышения безопасности работать можно с использованием резиновых ковров.

Важное значение для предотвращения электротравматизма имеет правильная организация обслуживания действующих электроустановок, проведение ремонтных, монтажных и профилактических работ.

4.4. Экологическая безопасность

4.4.1. Анализ влияния объекта исследования на окружающую среду

В результате выполнения работы были исследованы линейные последовательности при помощи регистра сдвига. Данное устройство не выделяет загрязнений способных навредить гидросфере или атмосфере, так как она работает на электрическом токе. Потенциальное загрязнение окружающей среды связано только с литосферой, которой может быть причинен вред при неправильной утилизации составных частей устройства. Однако объем производства устройства прямо пропорционально зависит от уровня энергетики. Развитие энергетической сферы оказывает существенное влияние на окружающую среду, так как является источником загрязнения гидросферы, атмосферы и литосферы, а также недр земной поверхности, ввиду потребления ископаемых ресурсов.

4.4.2. Обоснование мероприятий по защите окружающей среды

Основными источниками загрязнения окружающей среды являются отходы, образующиеся после окончания срока службы устройства управления. Отходы — это остатки продуктов или дополнительный продукт, образующиеся в процессе или по завершении определенной деятельности и не используемые в непосредственной связи с этой деятельностью [29]. Виды отходов:

- Отходы производства (остатки сырья, материалов, изделий и полуфабрикатов, а также иных продуктов и веществ, образовавшихся в ходе производственного процесса, выполнения ряда услуг или выработки энергии, бракованная продукция, материалы, утратившие свои прежние свойства);
- Отходы потребления (остатки предметов или вещей, утративших свои основные исходные свойства в результате использования или износа);
- Отходы потребления, образующиеся у населения, являются твердыми бытовыми отходами;
- Инертные отходы (отходы от упаковки из стекла, металла, бумаги, дерева, кожи, тканей);
- Опасные отходы. Существуют следующие виды отходов в зависимости от степени токсичности: чрезвычайно опасные (I), высокотоксичные (II), умеренно опасные (III) и малоопасные (IV). Токсичность отходов определяется содержанием опасных веществ, приводящих к самовозгоранию, реактивных веществ, канцерогенов и т.д.

Элементы устройства управления по окончании срока эксплуатации относятся к твердым бытовым отходам и должны быть утилизированы надлежащим образом в соответствующих местах утилизации отходов.

Утилизация полимерных отходов регламентируются стандартом [20]. Согласно этому стандарту, пластмассовый корпус устройства управления по истечению срока службы следует отправлять на переработку.

4.5. Безопасность в чрезвычайных ситуациях

Чрезвычайные ситуации относятся к совокупности опасных событий или явлений, приводящих к нарушению безопасности жизнедеятельности. Основными причинами возникновения чрезвычайных ситуаций являются: во-первых – внутренние, к которым относятся сложность технологий, недостаточная квалификация персонала, проектно-конструкторские недоработки, физический и моральный износ оборудования, низкая трудовая и технологическая дисциплина; во-вторых – внешние чрезвычайные ситуации (стихийные бедствия, неожиданное прекращение подачи электроэнергии, воды, технологических продуктов и т.д.).

4.5.1. Анализ вероятных ЧС, которые может инициировать объект исследований

Наиболее вероятной чрезвычайной ситуацией, которая может возникнуть при работе с прибором является пожар.

Причинами пожара могут быть:

- токи короткого замыкания;
- неисправность электросетей;
- незнание или небрежность обслуживающего персонала;
- курение в неположенных местах.

Пожарная безопасность предусматривает обеспечение безопасности людей и сохранения материальных ценностей предприятия на всех стадиях его жизненного цикла. Основными системами пожарной безопасности являются системы предотвращения пожара и противопожарной защиты, включая организационно-технические мероприятия. Пожарная профилактика – комплекс организационных и технических мероприятий, направленных на обеспечение безопасности людей, на предотвращение пожара, ограничение его распространения, а также на создание условий, на успешное тушение пожара. Успех борьбы с пожаром зависит от своевременного обнаружения пожара и быстрого принятия мер по его ликвидации. Исходя из установленной

номенклатуры обозначений зданий по степени пожарной опасности, анализируемое в данной работе помещение относится к категории В [31]. Среди организационных и технических мероприятий, осуществляемых для устранения пожара, необходимо выделять следующие меры:

- использование исправного оборудования, электропроводки;
- проведение инструктажей по пожарной безопасности;
- назначение ответственного за пожарную безопасность в помещениях предприятий, лабораториях учебных корпусов;
- наличие план эвакуации людей, который должен висеть на видном месте;
- курение в строго отведенном месте;
- содержание путей и проходов для эвакуации людей в свободном состоянии.

4.5.2. Обоснование мероприятий по предотвращению ЧС и разработка порядка действия в случае возникновения ЧС

В лабораторной комнате должны висеть огнетушители (углекислотные), а также силовой щит, который позволяет мгновенно обесточить его. Всякий работник при обнаружении пожара должен:

- незамедлительно сообщить о возгорании в городскую пожарную охрану по телефону 01 (с мобильного – 010) и оповестить руководство, если не сработала автоматическая система обнаружения пожара;
- принять меры по эвакуации людей, каких-либо материальных ценностей с использованием для этого имеющихся средств и сил;
- отключить электроэнергию,
- прекратить все работы в здании (если это допустимо по технологическому процессу производства), кроме работ, связанных с тушением пожара;
- удалить за пределы опасной зоны всех сотрудников, не участвующих в тушении пожара.

Вывод по разделу

В данном разделе было проведено исследование регистра сдвига с линейной обратной связью с точки зрения безопасности для окружающей среды и человека. Из данного исследования можно сделать вывод, что предложенный проект не несет высокой опасности для человека, а в случае соблюдения мер предосторожности, и для окружающей среды.

Заключение

В результате выполнения работы произвели исследование однородных линейных рекуррентных последовательностей над бинарным полем. Построили последовательности максимальной длины при помощи регистров сдвига с линейной обратной связью. Были проведены испытания при различных состояниях регистра сдвига, такие как: гистограмма распределения элементов, последовательности, распределение на плоскости, автокорреляционная функция, графический спектральный тест. В ходе этих испытаний было выявлено, что мы произвели правильный выбор примитивного полинома и начального состояния регистра, что доказывают результаты испытаний.

Были разработаны функциональная и принципиальная электрическая схема регистра сдвига с линейной обратной связью. Построена таблица генерации PN – последовательности максимальной длины.

По результатам выполненной работы была рассчитана смета затрат на выполнение проекта. В результате данных расчетов получили стоимость НИР равную 359 501,64 рублей.

Список использованных источников

1. Угрюмов Е. П. Цифровая схемотехника, – СПб.: БХВ – Санкт-Петербург, 2000. – 528 с.: ил.
2. Система современных технических вычислений Wolfram [Электронный ресурс]. Режим доступа: <https://www.wolfram.com/mathematica> (дата обращения: 25.05.2020).
3. Ларин А. Л. Основы цифровой электроники — М.: МФТИ, 2008. — 314 с. — ISBN 978-5-7417-0228-4
4. Белоус, А.И. Основы конструирования высокоскоростных электронных устройств: краткий курс «белой магии» / А.И. Белоус, В.А. Солодуха, С.В. Шведов; под общ. ред. А.И. Белоус. – Москва: Техносфера, 2017. – 872 с.: ил., табл., схем. – (Мир электроники).
5. Блейхут Ричард. Теория и практика кодов, контролирующих ошибки [Theory and Practice of Error Control Codes] — М.: Мир, 1986.
6. LFSR: генерация псевдослучайных чисел на регистре сдвига [Электронный ресурс]. Режим доступа: <http://microsin.net/programming/avr/lfsr-pseudo-random-number-generator.html> (дата обращения: 19.05.2020).
7. М. А. Иванов, И. В. Чугунков. Глава 4. Методика оценки качества генераторов ПСП // Теория, применение и оценка качества генераторов псевдослучайных последовательностей. — М.: КУДИЦ-ОБРАЗ, 2003. — 240 с. — ISBN 5-93378-056-1.
8. Б. Я. Рябко, А. И. Пестунов. «Стопка книг» как новый статистический тест для случайных чисел//Пробл. передачи информ.2004, том 40, выпуск 1, с. 73–78
9. А. И. Миненко. Экспериментальное исследование эффективности тестов для проверки генераторов случайных чисел// Вестник СибГУТИ.2010, No 4, с. 36-46.
10. ГОСТ Р ИСО 3534-1-2019 Статистические методы. Словарь и условные обозначения. Часть 1. Общие статистические термины и термины, используемые в теории вероятностей.
11. ГОСТ 21.208-2013. Система проектной документации для

строительства (СПДС). Автоматизация технологических процессов.
Обозначения условные приборов и средств автоматизации в схемах.

12. Конотопский В.Ю. Методические указания к выполнению раздела «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение» для всех специальностей / – Томск: Томский политехнический университет, 2015.

– 29 с.

13. ГОСТ 12.2.032-78. Система стандартов безопасности труда (ССБТ). Рабочее место при выполнении работ сидя. Общие эргономические требования.

14. ГОСТ 22269-76. Система «Человек-машина». Рабочее место оператора. Взаимное расположение элементов рабочего места. Общие эргономические требования.

15. ГОСТ 21889-76. Система «Человек-машина». Кресло человека оператора. Общие эргономические требования.

16. ГОСТ 21958-76. Система «Человек-машина». Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования.

17. Трудовой кодекс Российской Федерации [Электронный ресурс]: от 30.12.2001 №197-ФЗ (ред. от 01.04.2019) // Консультант Плюс: справочная правовая система. URL: http://www.consultant.ru/document/cons_doc_LAW_346

83/09dd7ce09d17960c4356ad42264f09db302f3fe0/ (дата обращения 02.05.2019).

18. СанПиН 2.2.4.3359-16. «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах».

19. ГОСТ 12.1.029-80. Система стандартов безопасности труда (ССБТ). Средства и методы защиты от шума. Классификация.

20. ГОСТ 12.1.038-82. Система стандартов безопасности труда (ССБТ). Электробезопасность. Предельно допустимые значения напряжений прикосновения и токов.

21. ГОСТ 12.1.002-84. Система стандартов безопасности труда (ССБТ). Электрические поля промышленной частоты. Допустимые уровни

напряженности и требования к проведению контроля на рабочих местах.

22. СанПиН 2.2.2/2.4.1340-03. «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

23. СанПиН 2.2.4.548-96. Гигиенические требования к микроклимату производственных помещений.

24. СНиП 41-01-2003. Отопление, вентиляция и кондиционирование.

25. СП 52.13330.2016. Естественное и искусственное освещение.

Актуализированная редакция СНиП 23-05-95*.

26. ГОСТ Р 12.1.019-2009. Система стандартов безопасности труда (ССБТ). Электробезопасность. Общие требования и номенклатура видов защиты.

27. Безопасность жизнедеятельности. Безопасность технологических процессов и производств. Охрана труда: учебное пособие для вузов / П.П.

Кукин и др. - 5-е изд., стер. - М.: Высшая школа, 2009. - 335 с.

28. ГОСТ 21.408-2013. Система проектной документации для строительства (СПДС). Правила выполнения рабочей документации автоматизации технологических процессов.

29. Классификация и утилизация твердых бытовых отходов [Электронный ресурс] URL: <http://metalspace.ru/education-career/osnovymetallurgii/tbo/923-tverdye-bytovye-otkhody.html>.

30. ГОСТ Р 54533-2011. «Ресурсосбережение. Обращение с отходами. Руководящие принципы и методы утилизации полимерных отходов»

31. НПБ 105-95. Определение категорий помещений и зданий по взрывопожарной и пожарной опасности, утв. Приказом ГУ ГПС МВД РФ от 31.10.95 № 32.

Приложение А

(обязательное)

Функциональная схема 16-разрядного регистра сдвига с линейной обратной связью



Рисунок А.1 – Функциональная схема 16-разрядного РСЛОС на основе примитивного полинома $x^{16} + x^5 + x^3 + x^2 + 1$

Приложение Б

(Обязательное)

Принципиальная схема регистра сдвига с линейной обратной связью

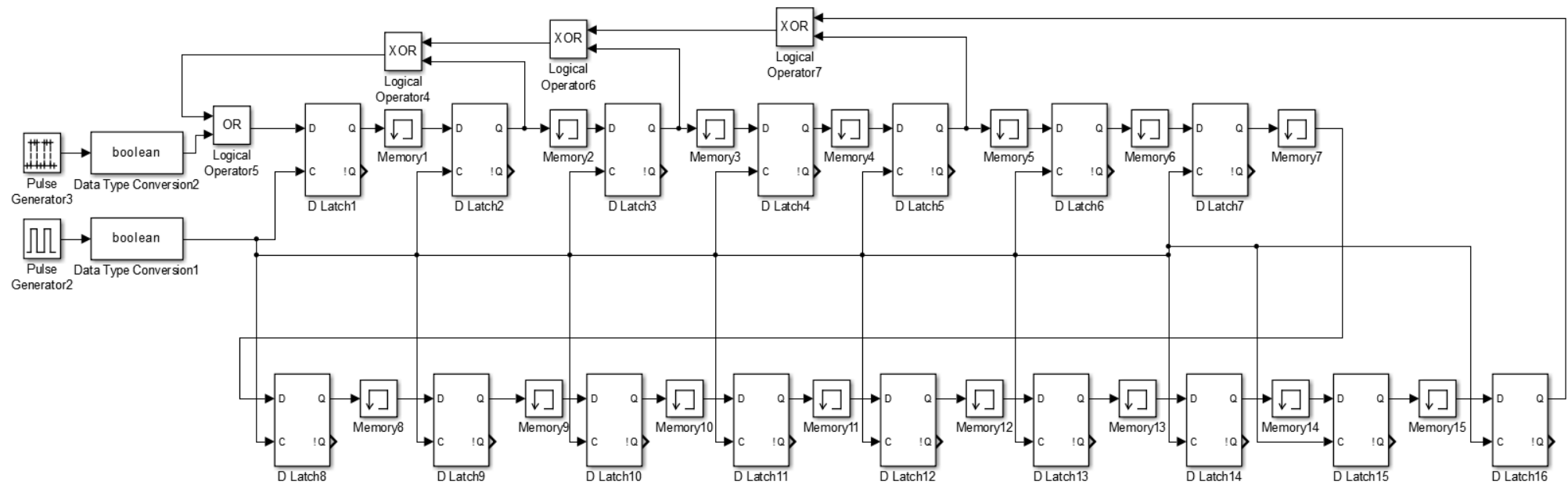


Рисунок Б.1 – Принципиальная схема 16-разрядного РСЛОС в среде симуляции Simulink Matlab

Приложение В

(Обязательное)

Таблица генерации бинарной последовательности

№ итерации	Выходная последовательность (16 разрядов)																Значение в 10- ричной системе
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
2	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	45
3	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	1	1105
4	1	0	1	1	1	1	0	1	1	0	1	0	1	1	0	1	48557
5	0	0	0	1	0	0	1	1	1	1	0	1	0	0	1	1	5075
6	1	0	1	1	1	0	0	0	0	1	1	1	0	1	1	1	47223
7	1	0	0	1	0	1	0	0	1	1	1	0	0	1	1	1	38119
8	1	1	1	1	1	1	0	0	1	0	1	1	1	0	0	0	64696
9	0	1	1	1	1	1	0	0	1	0	0	1	0	1	0	1	31893
10	1	1	1	1	1	0	0	0	1	1	0	1	0	0	1	0	63698
11	1	1	0	0	0	1	1	1	0	1	0	1	0	1	1	1	51031
12	0	0	0	0	1	0	1	0	0	1	0	1	0	0	1	0	2642
...
65536	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
65537	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	45
65538	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	1	1105
65539	1	0	1	1	1	1	0	1	1	0	1	0	1	1	0	1	48557
...

Приложение Г

(Обязательное)

Гистограмма распределения элементов последовательности

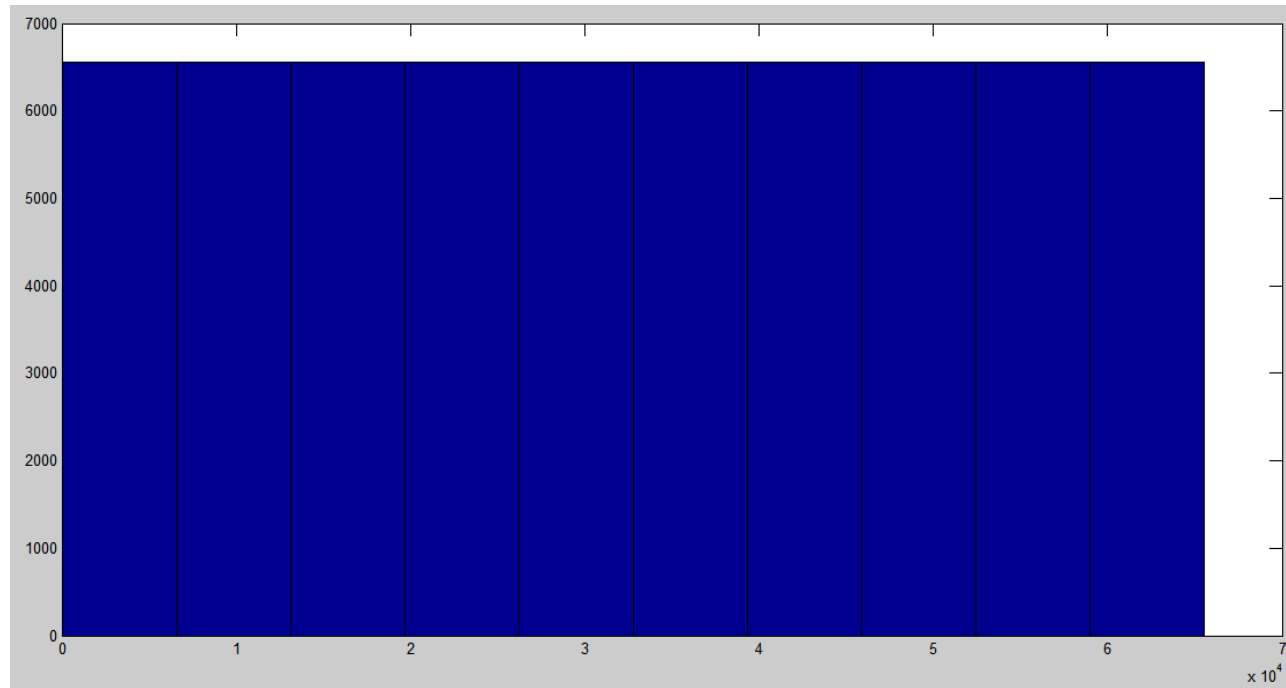


Рисунок Г.1 – Гистограмма распределения сгенерированной 16-разрядным РСЛОС *PN*-последовательности

Приложение Д

(Обязательное)

Распределение на плоскости

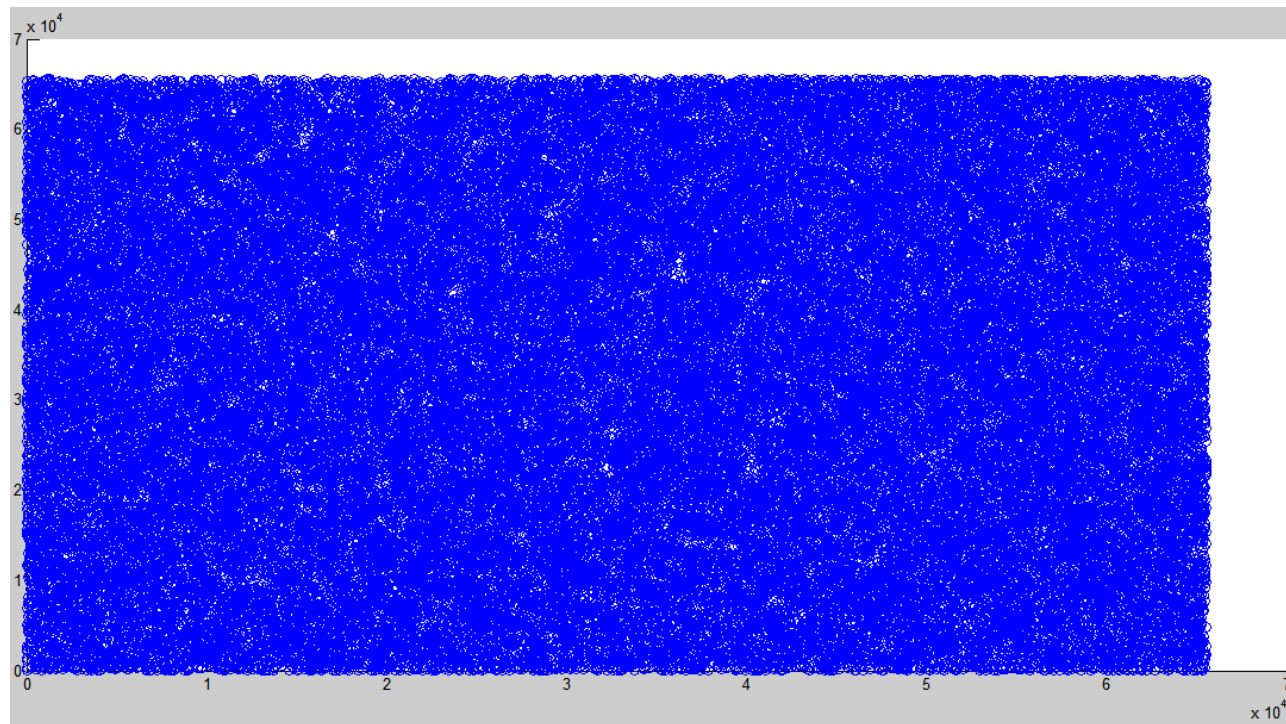


Рисунок Д.1 – Распределение на плоскости сгенерированной 16-разрядным РСЛОС *PN*-последовательности

Приложение Е

(Обязательное)

Автокорреляционная функция

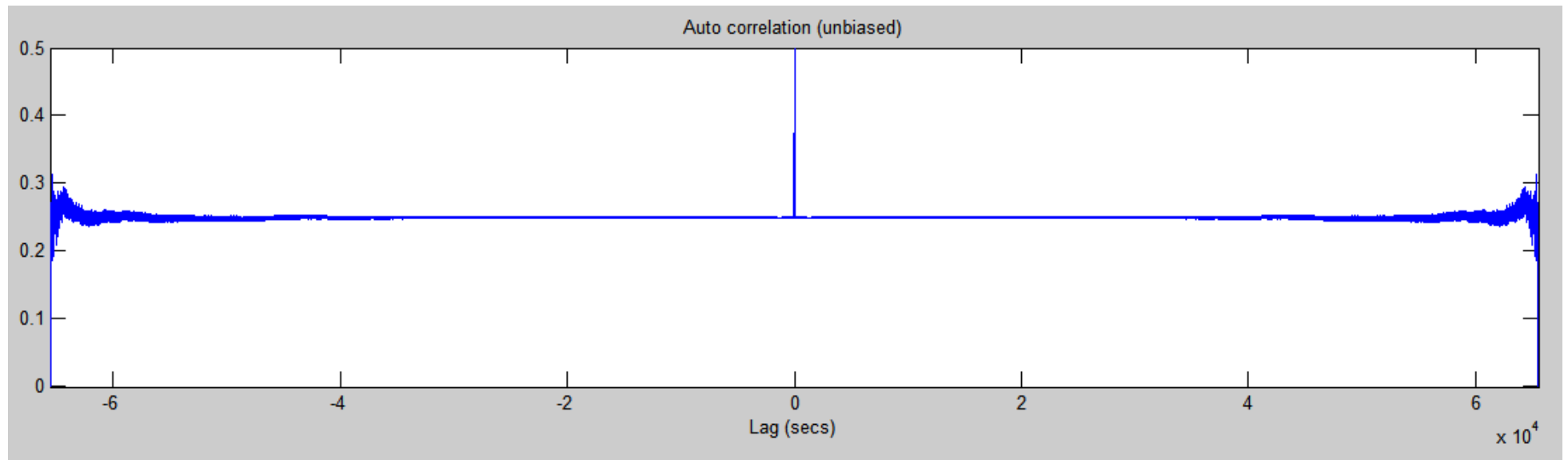


Рисунок Е.1 – Автокорреляционная функция сгенерированной 16-разрядным РСЛОС *PN*-последовательности

Приложение Ж

(Обязательное)

Графический спектральный тест

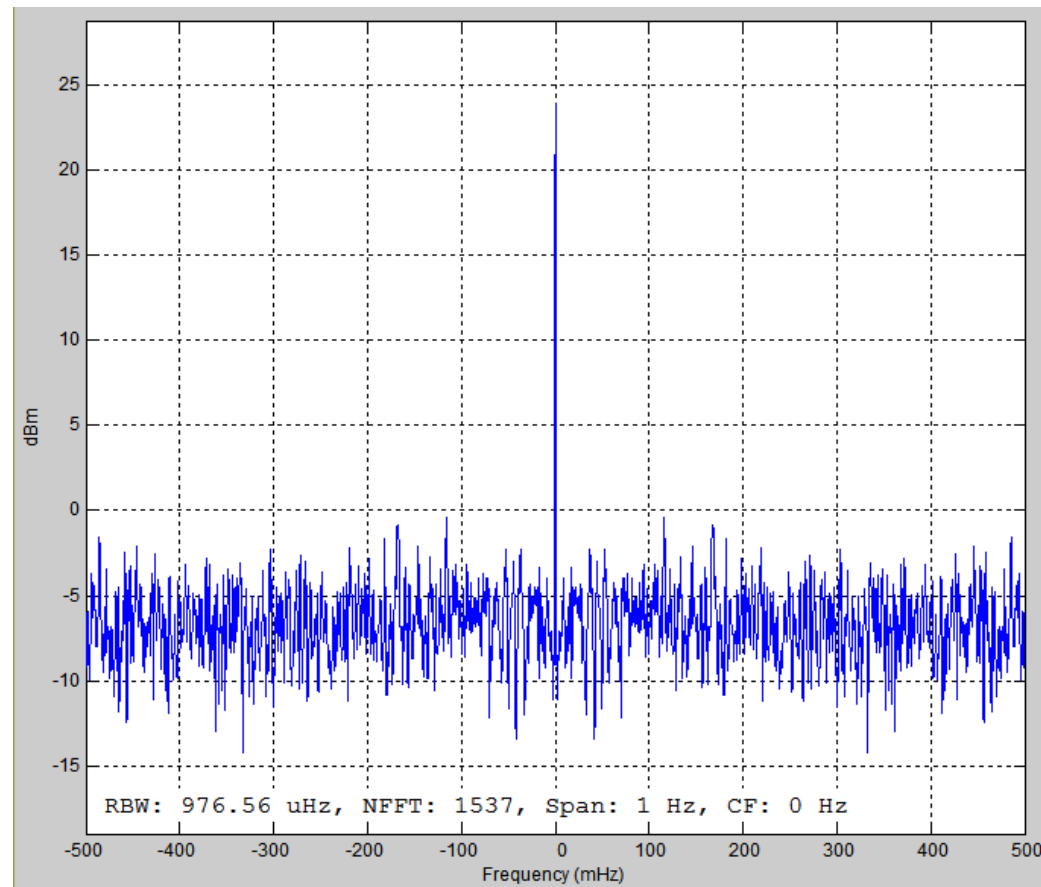


Рисунок Ж.1 – Графический спектральный тест сгенерированной 16-разрядным РСЛОС *PN*-последовательности